

**S. 809, ONLINE PRIVACY PROTECTION ACT OF
1999**

HEARING

BEFORE THE
SUBCOMMITTEE ON COMMUNICATIONS
OF THE
COMMITTEE ON COMMERCE,
SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE
ONE HUNDRED SIXTH CONGRESS
FIRST SESSION

—————
JULY 27, 1999
—————

Printed for the use of the Committee on Commerce, Science, and Transportation



U.S. GOVERNMENT PRINTING OFFICE

71-813 PDF

WASHINGTON : 2002

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

JOHN McCAIN, Arizona, *Chairman*

TED STEVENS, Alaska	ERNEST F. HOLLINGS, South Carolina
CONRAD BURNS, Montana	DANIEL K. INOUE, Hawaii
SLADE GORTON, Washington	JOHN D. ROCKEFELLER IV, West Virginia
TRENT LOTT, Mississippi	JOHN F. KERRY, Massachusetts
KAY BAILEY HUTCHISON, Texas	JOHN B. BREAU, Louisiana
OLYMPIA J. SNOWE, Maine	RICHARD H. BRYAN, Nevada
JOHN ASHCROFT, Missouri	BYRON L. DORGAN, North Dakota
BILL FRIST, Tennessee	RON WYDEN, Oregon
SPENCER ABRAHAM, Michigan	MAX CLELAND, Georgia
SAM BROWNBACK, Kansas	

MARK BUSE, *Policy Director*

MARTHA P. ALLBRIGHT, *General Counsel*

IVAN A. SCHLAGER, *Democratic Chief Counsel and Staff Director*

KEVIN D. KAYES, *Democratic General Counsel*

SUBCOMMITTEE ON COMMUNICATIONS

CONRAD BURNS, Montana, *Chairman*

TED STEVENS, Alaska	ERNEST F. HOLLINGS, South Carolina
SLADE GORTON, Washington	DANIEL K. INOUE, Hawaii
TRENT LOTT, Mississippi	JOHN F. KERRY, Massachusetts
JOHN ASHCROFT, Missouri	JOHN B. BREAU, Louisiana
KAY BAILEY HUTCHISON, Texas	JOHN D. ROCKEFELLER IV, West Virginia
SPENCER ABRAHAM, Michigan	BYRON L. DORGAN, North Dakota
BILL FRIST, Tennessee	RON WYDEN, Oregon
SAM BROWNBACK, Kansas	MAX CLELAND, Georgia

CONTENTS

	Page
Hearing held July 27, 1999	1
Statement of Senator Bryan	4
Statement of Senator Burns	1
Statement of Senator Dorgan	25
Prepared statement	25
Statement of Senator Kerry	3
Statement of Senator Rockefeller	26
Statement of Senator Stevens	5
Statement of Senator Wyden	24
WITNESSES	
Anthony, Sheila F., commissioner, Federal Trade Commission	26
Prepared statement	29
Lesser, Jill, vice president, Domestic Public Policy, America Online	46
Prepared statement	48
Mulligan, Deirdre, staff counsel, Center for Democracy and Technology	52
Prepared statement	54
Pitofsky, Robert, chairman, Federal Trade Commission	5
Prepared statement	7
Rotenberg, Marc, director, Electronic Privacy Information Center	64
Swindle, Orson, commissioner, Federal Trade Commission	29
Prepared statement	31
Thompson, Mozelle W., commissioner, Federal Trade Commission	32
Varney, Christine, senior partner, Hogan & Hartson, on behalf of the Online Privacy Alliance	66
Prepared statement	68
APPENDIX	
Center for Democracy and Technology prepared statement	87

S. 809, PRIVACY PROTECTION ACT OF 1999

TUESDAY, JULY 27, 1999

U.S. SENATE,
SUBCOMMITTEE ON COMMUNICATIONS,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The subcommittee met, pursuant to notice, at 9:30 a.m. in room SR-253, Russell Senate Office Building, Hon. Conrad Burns, chairman of the subcommittee, presiding.

Staff members assigned to this hearing: Robert Taylor, Republican counsel; Moses Boyd, Democratic senior counsel; and Al Mottur, Democratic counsel.

OPENING STATEMENT OF HON. CONRAD BURNS, U.S. SENATOR FROM MONTANA

Senator BURNS. We will call the committee to order this morning. I will tell you, it has been a long day already. I started off at Bethesda Naval Hospital this morning, and we chaired and then completed a MILCON appropriations, now we have got this, and I will have all my work done by noon, and then I am going to go to the golf course. [Laughter.]

Today's hearing concerns a topic of critical importance to today's increasingly digital world, the protection of online privacy. The recent growth of the Internet has been nothing short of breathtaking. The number of Internet users in the United States is now approaching 100 million. The number of online consumers is now over 30 million. Clearly, the Internet has become a staple of everybody's life.

The tremendous reach of the Internet does pose challenges as well as opportunities. Just as the revolution in communications technology has allowed individuals to gain access to nearly limitless information, unfortunately digital technologies can also be used by bad actors to collect nearly limitless information on individuals with out their knowledge.

I would like to thank my good friend and colleague, Senator Wyden, for his vision and hard work in working with me on the Online Privacy Protection Act of 1999, which will ensure the safety net for privacy for online consumers.

I have worked closely with Senator Wyden in a bipartisan manner on numerous high tech issues, and we continue to do that. I know he shares my hesitation to engage in any sort of regulation of the Internet, but nonetheless we see a problem looming on the horizon. I have stated on many occasions that nothing happens

until a sale is made and the intent of this bill is to foster, not impede, the tremendous growth in electronic commerce.

This bill was a product of many discussions with both industry and privacy groups, and represents a balanced measured approach to the issue. We are very fortunate to have the entire Federal Trade Commission here today. I would especially like to thank the chairman for altering his very demanding schedule to be here today. I have worked very closely with the chairman on matters of Internet privacy in the past, and last year the Children's Online Privacy Protection Act, which I supported, drew heavily from the recommendations and the findings of the FTC's June 1998 report on Internet privacy.

The 1998 report found that 89 percent of children's Web sites collected personal information, while only 10 percent of the sites provided for some form of parental control over the collection and use of that information.

Thanks to the recommendations of the FTC and the work of Senator McCain and Senator Bryan and other members of the Commerce Committee, the Children's Online Privacy Protection Act, which requires the FTC to come up with some rules that would provide notice of Web sites personal information collection, passed into law in the 105th Congress.

Now, given this background, I have to say that I am very puzzled by the FTC's recent report to Congress on Internet privacy. The report acknowledged that fewer than 10 percent of the Web sites meet basic privacy protections, but called for no Federal legislation to address this critical situation.

The report pointed to the recent Georgetown study that shows that nearly two-thirds of Web sites now post privacy policies as proof of industry progress and a reason for legislation inaction. I applaud the increase in posting privacy policies, but what about the other kinds of Web sites that fail to inform the consumers?

Also, I have examined several of these policies. Many of them seem to have the purpose of exempting Web sites from liability, rather than informing consumers of their rights. The fact that many of these policies require a law degree to decipher, not to mention a magnifying glass, given that they are in microscopic type, does not lead me to the conclusion that no Federal action is necessary to protect online privacy.

I find the dissenting opinion of Commissioner Anthony in the report very compelling. She rightly states that the legislation is necessary to at least ensure a minimum of consumer privacy protection in the digital era. In her opinion, her expression concerns that the absence of effective privacy protections will undermine consumer confidence and hinder the advancement of electronic commerce and trade, and I could not agree more.

In fact, several recent studies reveal that the single greatest reason consumers do not buy goods online is because of the concerns of privacy. Unfortunately, these fears have been proven to be well-based. As the communications revolution alters every aspect of our personal and economic lives, now is no time for delay or inaction.

I continue to move forward with this critical bill to make sure that consumers can feel confident in the safety of their personal information in the digital age. It is nice to work with Senator Wyden

and my colleagues on the committee to ensure this bill moves to markup and passage by the full Senate as quickly as possible.

I see my good friend from Massachusetts here this morning, and thank you for coming, Senator, and we look forward to your statement.

**STATEMENT OF HON. JOHN F. KERRY, U.S. SENATOR
FROM MASSACHUSETTS**

Senator KERRY. Thank you very much, Mr. Chairman. I will be very brief. I can only stay for a portion of the hearing, but I wanted to first of all thank you for having this hearing. This is a complex and very important issue to all of us, and I will just be very, very brief, as I said.

A lot of us have been taking time to meet with a lot of the companies and begin to understand better what is happening in the marketplace. I think we are beginning to get that sense. It strikes me that obviously privacy is going to grow. I think most people I have talked with in the industry are aware of that, it will grow as an issue and be vital to the capacity of many companies to be able to market and to grow. I think people understand that.

I have looked at the FTC's report on privacy, and generally agree with most of the majority view, though I think, as you just said, Mr. Chairman, that Commissioner Anthony's warnings and observations are not to be discounted.

Many Web sites are currently taking steps to notify users of their privacy programs, and I think we are at significantly enough of a nascent stage of development here that I am wary of regulation at this point in time. I do not think it is the right time to regulate the industry. I think, however, the FTC may have somewhat overstated to some degree the progress that is currently being made.

There is a marked improvement in the number of sites posting privacy disclosure, but disclosure is different from the set of choices sites have with respect to all the things they could do to protect privacy.

The studies that you referenced, and that the report references, show that only 10 percent of the sites are currently addressing the four principles of notice, choice, access, and security. I think that 10 percent figure should concern all of us, but again, that is different from whether or not at this point in time we ought to step in and actually regulate.

I think it probably concerns a lot of other people, too, and we ought to simply hold out our own notice to all of the participants that we are going to be watching very closely. We should set high standards at this point in time as a goal for them to achieve.

But again, I think self-regulation is the more important way to proceed at this point in time. I am not sure that we or the FTC could write a law or regulation that will sufficiently allow for all the changes in technology that are taking place, and again, I am absolutely convinced that the companies understand that protecting consumer privacy is in their best interests, and with the level of competition on the Web right now, I think we would be well-advised to allow that to sort of percolate a little bit and perhaps see where we are.

So that said, Mr. Chairman, I think if self-regulation is not working, and the surveys continue to show only minimal compliance with the core privacy principles, we certainly have ample opportunity to step in at that time, and I thank you again, Mr. Chairman, for setting us down this road.

Senator BURNS. Thank you, Senator Kerry.
Senator Bryan.

**STATEMENT OF HON. RICHARD H. BRYAN, U.S. SENATOR
FROM NEVADA**

Senator BRYAN. Thank you very much, Mr. Chairman. Let me first preface my comments by commending you for holding this hearing and the leadership that you and our colleague, Senator Wyden, have provided on this issue.

I think Business Week magazine summed it up best in its July 26 article:

“George Orwell’s vision of Big Brother was Government run amok, but it is not Government that threatens privacy today, it is Internet commerce.”

That is a Business Week publication.

Internet commerce is evolving to the point where you could be browsing a Web page for mutual funds at one moment and seconds later get a call from a telemarketer with a targeted mutual fund sales pitch. As online commerce grows, the value of personal information for direct marketing will skyrocket. As Business Week put it, all over the Web a data gold rush is on. The incredible communications and computing power of the Internet is handing companies an unprecedented opportunity to collect and analyze information.

As some of you will recall, I became involved in the Internet privacy issue in the last session of Congress, working with the chairman of the committee, Senator McCain, on the Child Online Privacy Protection Act. Working with the FTC, private sector groups as well, we were astonished to learn that Web sites that focused on children’s issues, and there were some 90 percent or more who were collecting personal and private data, only about 1 percent of those actually gave parents an opportunity to in effect have an informed consent.

Working with the private sector and the FTC, we have now developed the Child Online Privacy Protection Act. The rulemaking process is continuing, but the issue before us today is whether or not we should expand those privacy protections to the adult Internet population.

I have not rushed to judgment as the FTC reviews this issue, but, Mr. Chairman, let me express my concern. I think the privacy issue is very deep and very fundamental, and the American public is just beginning to grasp how threatened their concept of privacy is.

Although the industry needs to be commended for the strides it has made in setting up mechanisms to protect consumers’ privacy, I continue to be concerned about several practices. There appears to be an agreement that the biggest impediment to commerce on the Internet is the public concern about privacy, and so you have on one hand an issue in which the public is concerned about the loss of privacy, the business community, which is interested in ex-

panding the potential for e-commerce, is impeded because of those customers' concerns that the transaction over the Internet will invade their privacy to an extent that they do not feel comfortable with.

Of the top 100 Web sites, 99 collect personal information, but only 22 meet the fair information practice standards that have been outlined. While we are focusing on privacy protection for information consumers voluntarily give to the Web sites, that is when they have a transaction much like an individual who walks into a retail establishment and produces his or her credit card or pays in cash, there is a record of that transaction. I think all of us understand that concept.

But a device known as cookies, cookies I think is something that would shock people. That is, it is now possible through this amazing technology for a Web site to know when it has been visited, not when a transaction has occurred, but when a Web site has been visited, that information collected and made available for direct marketers without the knowledge or the consent of the consumer.

That, Mr. Chairman, in my judgment raises significant concerns, so it is my hope that the industry and the regulators will be able to work out something that will protect this privacy. I must tell you, I am not persuaded at this point that that is the case. I know the FTC has urged caution and restraint at this moment.

Mr. Chairman, I commend you again for your leadership in moving this ball forward. I think there is a significant issue there, and that we may, indeed, have to resort to a legislative solution if we are not able to reach an agreement very soon in terms of how we protect adult users of the Internet, and I thank you, Mr. Chairman.

Senator BURNS. Thank you, Senator Bryan.

Senator Stevens.

Senator STEVENS. No opening statement.

Senator BURNS. Well, we welcome the Federal Trade Commission this morning, and the chairman, and we will hear first from the chairman, Mr. Robert Pitofsky, and we welcome you this morning and thank you for coming en masse, we might add. We like that idea.

**STATEMENT OF HON. ROBERT PITOFSKY, CHAIRMAN,
FEDERAL TRADE COMMISSION**

Mr. PITOFSKY. Thank you very much, Mr. Chairman, and members of the committee. It is truly a pleasure to meet with this group that is so knowledgeable about the problems that we are going to address, the development of the Internet and privacy issues on the Internet.

Let me try to focus the discussion in this way. Members of the FTC are unanimous, and I believe the members of this committee are probably unanimous, that it is absolutely intolerable for sellers on the Internet to gather personally identifiable information and sell it or otherwise transfer it without the buyer's permission. We are all there. The question is, what is the best way to ensure that that kind of behavior does not occur?

My own view is that there are always going to be four different elements to a regulatory program of this sort. One, case by case enforcement based on statutes already existing, like our own statute

that outlaws deception; new legislation, consumer education, and self-regulation. The question is, what is the right mix to get to the goal line?

The FTC has taken a leadership role in this area. We have brought a number of cases challenging violations of consumer privacy on the Internet. We sued Geo Cities, one of the biggest cases that we have seen in this area, and we have brought other suits. We have supported legislation. Indeed, we worked with this committee and particularly the chairman and Mr. Bryan on the Children's Online Privacy Act, which was put through the Congress in the most efficient and prompt way that I think I have ever seen.

We last week unanimously testified in favor of legislation that would protect the privacy of financial records, because financial records are different and deserve a heightened level of privacy protections. I would say the same thing about medical records.

But the issue remains, what do we do about all the rest of the invasions of privacy that adults may encounter when they do business on the Internet, and to address that, let me talk a little bit about history. The FTC got out in front of this issue with hearings that were held 3 years ago examining questions of the extent of invasions of privacy and what to do about it. We then did a study at the request of Senator McCain, addressing questions such as what are the levels of invasion of privacy, and what are the existing protections. In the summer of 1998 we put out a report.

We submitted a report to the Congress that said that, even though practically everyone was collecting personally identifiable information, only 14 percent posted any sort of notice, and only 2 percent touched all the bases—that is: notice, consent, access, and security, and we said at that time as politely as we knew how that this was a very disappointing performance by the private sector.

Industry then agreed with that assessment, and the most responsible companies in this country working on the Internet said, give us a chance to solve this problem through self-regulation, and they have put in considerable time and effort and resources to accomplish that.

Georgetown University then ran a study about a year later, and found that the 14 percent policy disclosures had become 66 percent. I myself was astonished that in 1 year, disclosures increased from 14 percent to 66 percent. Indeed, a second study which looked only at the most frequently used Internet sites had the disclosure policies up around 80 or 81 percent.

Still, only 10 percent, another study said 20 percent, but I say only 10 percent touched all the bases, and therefore while you have notice and opportunities to opt out, you do not have the access issue taken care of, and you do not have the security issue taken care of.

The question is, what do we do now? We are at a very important crossroads point in time as to what is the best way to address these questions. One is to let self-regulation proceed, and industry is following up to improve their performance. For example, I know they sent a letter to the 34 percent of the sites on the Internet that did not have privacy policies, asked them why, and urged them to change their policies. If the private sector were to have anything like the success this year that I had last year with self-regulation,

you would be up around 90 or 95 percent of disclosure of policy and remember, once they disclose their policies, if they do not abide by their own policy, that is deceptive under our statute and we can challenge their behavior under section 5 of the Federal Trade Commission Act.

Of course, we could now move to a law, and I must say that if we were to move to a law, the direction described in S. 809, not every single word in the statute, of course, but the direction seems about right to me. By the way, S. 809 pretty much reflects the direction that the business community has itself agreed to. That is to say, it calls for notice, consent, access, security, and safe harbors for those responsible companies that behave in the appropriate way.

A majority of the commission believes that we ought to let a little time go by, and I really mean a little time. There has been such progress, we challenged them so directly, and they came through in improving self-regulation so substantially that we ought to let a little time go by and see if they really get to the goal line.

If they do, then we have solved the problem without the necessity of legislation in an area that is so dynamic that one can only worry that the legislation will be outstripped by technological developments.

If they do not, if the progress does not proceed, then I would be the first to be up here recommending that legislation is necessary to accomplish what we agree is a necessary protection for consumers. So in the end consumers must be protected. It is just an issue of how you get there.

Now, a large part of the complexity of this depends on the following. Do you look at the 66 percent, say the glass is more than half full, and we are going in the right direction, or do you look at the disappointing 10 or 20 percent that have not touched all the bases?

I feel you should look at both. I do not think notice and opt-out is a successful addressing of this problem, but I will point out that Alan Weston, one of the most respected advocates for privacy policy in this country, released the results of a new study just about a week or 10 days ago. It showed that 85 percent of consumers principally or exclusively care about notice and consent, the 66 percent, and they really are not nearly as concerned, or not concerned at all, about, touching all four bases of security and access.

So while I think consumers are entitled to more than notice, it may be that many consumers really do not regard that as a priority issue for themselves, and it makes sense, because if you opt out, why do you have to worry about access? You are out of the system. If you opt out, why do you have to worry about security? The information gatherer cannot use your personal data, and if they do, after you have opted out, that would be a violation of our statute.

Thank you very much, and let me turn the program over to my colleagues.

[The prepared statement of Mr. Pitofsky follows:]

PREPARED STATEMENT OF ROBERT PITOFSKY, CHAIRMAN, FEDERAL
TRADE COMMISSION

Mr Chairman and members of the Subcommittee, I am Robert Pitofsky, Chairman of the Federal Trade Commission ("FTC" or "Commission"). I appreciate this oppor-

tunity to present the Commission's views on the progress of self-regulation in the area of online privacy.¹

I. INTRODUCTION AND BACKGROUND

The FTC's mission is to promote the efficient functioning of the marketplace by protecting consumers from unfair or deceptive acts or practices and to increase consumer choice by promoting vigorous competition. As you know, the Commission's responsibilities are far-reaching. The Commission's primary legislative mandate is to enforce the Federal Trade Commission Act ("FTCA"), which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.² With the exception of certain industries, the FTCA provides the Commission with broad law enforcement authority over entities engaged in or whose business affects commerce³ and with the authority to gather information about such entities.⁴ Commerce on the Internet falls within the scope of this statutory mandate.⁵

In June 1998 the Commission issued Privacy Online: 24 Report to Congress ("1998 Report"), an examination of the information practices of commercial sites on the World Wide Web and of industry's efforts to implement self-regulatory programs to protect consumers' online privacy.⁶ Based in part on its extensive survey of over 1400 commercial Web sites, the Commission concluded that effective self-regulation had not yet taken hold.⁷ The Commission recommended that Congress adopt legislation setting forth standards for the online collection of personal information from children; and indeed, just four months after the 1998 Report was issued, Congress enacted the Children's Online Privacy Protection Act of 1998.⁸ As required by the Act, on April 20, 1999, the Commission issued a proposed Children's Online Privacy Protection Rule, which will implement the Act's fair information practices standards for commercial Web sites directed to children under 13, or who knowingly collect personal information from children under 13.⁹ Commission staff is reviewing comments on the proposed rule and will issue a final rule this fall.

When the 1998 report was released, there were indications that industry leaders were committed to work toward self-regulatory solutions. As a result, in Congressional testimony last July the Commission deferred judgment on the need for legislation to protect the online privacy of consumers generally, and instead urged industry to focus on the development of broad-based and effective self-regulatory programs.¹⁰ In the ensuing year, there have been important developments both in the growth of the Internet as a commercial marketplace and in consumers' and industry's responses to the privacy issues posed by the online collection of personal information. As you know, on July 13, 1999, the Commission issued a new report on these developments, Self-Regulation and Online Privacy: A Report to Congress (June 1999) ("1999 Report").¹¹

The 1999 Report notes that, while industry leaders have demonstrated substantial effort and commitment to privacy protections online, much remains to be done to ensure the widespread adoption and implementation of fair information practices. As a result, the Commission has developed an agenda for the coming months to assess the progress of self-regulation in greater detail. For these reasons, the Report concludes that legislation to address online privacy is not appropriate at this time. Nonetheless, I want to briefly present the Commission's views on S. 809, entitled the "Online Privacy Protection Act of 1999," which sets out one model to consider if there were to be legislation in the future.

S. 809 would require commercial Web sites to implement a framework of privacy protections that reflects the core fair information practices of notice, choice, access, and security. The bill combines government enforcement with incentives for effective self-regulation to protect consumers' online privacy.¹² It encourages industry participation in the process of developing information practice standards. The bill's safe harbor provision allows industry groups the flexibility to craft information practice guidelines that are sensitive to sector-specific concerns and technological developments, and to submit those guidelines for government approval. Once guidelines are approved, companies adhering to the guidelines are deemed in compliance with the bill's requirements as well. Because it reflects fair information practices and contains significant incentives for self-regulation, S. 809 would be a useful template for any online privacy legislation. We are pleased to work with the Committee as it continues to examine online privacy protections.

II. THE CURRENT STATE OF ONLINE PRIVACY REGULATION

The Commission's 1999 Report assesses the progress made in self-regulation to protect consumers' online privacy since last June and sets out an agenda of Commission actions in the coming year to encourage industry's full implementation of online

privacy protections. I am pleased to present the 1999 Report's findings to the Committee.

The Commission believes that self-regulation is the least intrusive and most efficient means to ensure fair information practices online, given the rapidly evolving nature of the Internet and computer technology. During the past year the Commission has been monitoring self-regulatory initiatives, and the Commission's 1999 Report finds that there has been notable progress. Two new industry-funded surveys of commercial Web sites suggest that online businesses are providing significantly more notice of their information practices than they were last year. Sixty-six percent of the sites in the Georgetown Internet Privacy Policy Survey ("GIPPS")¹³ post at least one disclosure about their information practices.¹⁴ Forty-four percent of these sites post privacy policy notices.¹⁵ Although differences in sampling methodology prevent direct comparisons between the GIPPS findings and the Commission's 1998 results,¹⁶ the GIPPS Report does demonstrate the real progress industry has made in giving consumers notice of at least some information practices. Similarly, 93% of the sites in the recent study commissioned by the Online Privacy Alliance ("OPA Study") provide at least one disclosure about their information practices.¹⁷ This, too, represents continued progress since last year, when 71% of the sites in the Commission's 1998 "Most Popular" sample posted an information practice disclosure.¹⁸

The new survey results show, however, that, despite the laudable efforts of industry leaders, significant challenges remain. The vast majority of the sites in both the GIPPS and OPA surveys collect personal information from consumers online.¹⁹ By contrast, only 10% of the sites in the GIPPS sample,²⁰ and only 22% of the sites in the OPA study,²¹ are implementing all four substantive fair information practice principles of Notice/Awareness, Choice/Consent, Access/Participation, and Security/Integrity.²² In light of these results, the Commission believes that further improvement is required to effectively protect consumers' online privacy.

In the Commission's view, the emergence of online privacy seal programs is a particularly promising development in self-regulation. Here, too, industry faces a considerable challenge. TRUSTe, launched nearly two years ago, currently has more than 500 licensees representing a variety of industries.²³ BBBOnline, a subsidiary of the Council of Better Business Bureaus, which launched its privacy seal program for online businesses last March, currently has 54 licensees and more than 300 applications for licenses.²⁴ Several other online privacy seal programs are just getting underway.²⁵ Together, the online privacy seal programs currently encompass only a handful of all Web sites. It is too early to judge how effective these programs will ultimately be in serving as enforcement mechanisms to protect consumers' online privacy.

III. CONCLUSION

The self-regulatory initiatives discussed above, and described in greater detail in the 1999 Report, reflect industry leaders' substantial effort and commitment to fair information practices. They should be commended for these efforts.

In addition, companies like IBM, Microsoft and Disney, which have recently announced, among other things, that they will forgo advertising on sites that do not adhere to fair information practices should be recognized for their efforts, which we hope will be emulated by their colleagues. Similarly, the Direct Marketing Association (DMA) is now requiring its members to follow a set of consumer privacy protection practices, including providing notice and an opportunity to opt-out, when identifying information is shared with other marketers, and to use the DMA's two national services for removing consumers' names from marketing lists.¹¹¹ Enforcement mechanisms that go beyond self-assessment are also gradually being implemented by the seal programs. Only a small minority of commercial Web sites, however, have joined these programs to date. Similarly, although the results of the GIPPS and OPA studies show that many online companies now understand the business case for protecting consumer privacy, they also show that the implementation of fair information practices is not widespread among commercial Web sites.

As stated previously, the Commission believes that legislation to address online privacy is not appropriate at this time. Yet, we also believe that industry faces some substantial challenges. Specifically, the present challenge is to educate those companies which still do not understand the importance of consumer privacy and to create incentives for further progress toward effective, widespread implementation.

First, industry groups must continue to encourage widespread adoption of fair information practices. Second, industry should focus its attention on the substance of web site information practices, ensuring that companies adhere to the core privacy principles discussed earlier. It may also be appropriate, at some point in the future,

for the FTC to examine the online privacy seal programs and report to Congress on whether these programs provide effective privacy protections for consumers.

Finally, industry must work together with government and consumer groups to educate consumers about privacy protection on the Internet. The ultimate goal of such efforts, together with effective self-regulation, will be heightened consumer acceptance and confidence. Industry should also redouble its efforts to develop effective technology to provide consumers with tools they can use to safeguard their own privacy online.

The Commission has developed an agenda to address online privacy issues throughout the coming year as a way of encouraging and, ultimately, assessing further progress in self-regulation to protect consumer online privacy:

- The Commission will hold a public workshop on “online profiling,” the practice of aggregating information about consumers’ preferences and interests gathered primarily by tracking their movements online. The workshop, jointly sponsored by the U.S. Department of Commerce, will examine online advertising firms’ use of tracking technologies to create targeted, user profile-based advertising campaigns.

- The Commission will hold a public workshop on the privacy implications of electronic identifiers that enhance Web sites’ ability to track consumers’ online behavior.

- In keeping with its history of fostering dialogue on online privacy issues among all stakeholders, the Commission will convene task forces of industry representatives and privacy and consumer advocates to develop strategies for furthering the implementation of fair information practices in the online environment.

One task force will focus upon understanding the costs and benefits of implementing fair information practices online, with particular emphasis on defining the parameters of the principles of consumer access to data and adequate security.

A second task force will address how incentives can be created to encourage the development of privacy-enhancing technologies, such as the World Wide Web Consortium’s Platform for Privacy Preferences (P3P).

- The Commission, in partnership with the U.S. Department of Commerce, will promote private sector business education initiatives designed to encourage new online entrepreneurs engaged in commerce on the Web to adopt fair information practices.

- Finally, the Commission believes it is important to continue to monitor the progress of self-regulation, to determine whether the self-regulatory programs discussed in the 1999 Report fulfill their promise. To that end, the Commission will conduct an online survey to reassess progress in Web sites’ implementation of fair information practices, and will report its findings to Congress.

The Commission is committed to the goal of full implementation of effective protections for online privacy in a manner that promotes a flourishing online marketplace, and looks forward to working with the Subcommittee as it considers the Commission’s 1999 Report.

ENDNOTES

1. The Commission vote to issue this testimony was 3–1, with Commissioner Anthony concurring in part and dissenting in part Commissioner Anthony’s statement is attached to the testimony. My oral testimony and responses to questions you may have reflect my own views and are not necessarily the views of the Commission or any Commissioner.

2. 15 U.S.C. § 45(a).

3. The Commission does not have criminal law enforcement authority. Further, certain entities, such as banks, savings and loan associations, and common carriers, as well as the business of insurance are wholly or partially exempt from Commission jurisdiction. See Section 5(a)(2) of the FTC Act, 15 U.S.C. § 45(a)(2), and the McCarran-Ferguson Act, 15 U.S.C. § 1012(b).

4. 15 U.S.C. § 46(a). However, the Commission’s authority to conduct studies and prepare reports relating to the business of insurance is limited. According to 15 U.S.C. § 46(a): “The Commission may exercise such authority only upon receiving a request which is agreed to by a majority of the members of the Committee on Commerce, Science, and Transportation of the Senate or the Committee on Energy and Commerce of the House of Representatives. The authority to conduct any such study shall expire at the end of the Congress during which the request for such study was made.”

The Commission also has responsibility under approximately forty additional statutes governing specific industries and practices. These include, for example, the

Truth in Lending Act, 15 U.S.C. §§ 1601 *et. seq.*, which mandates disclosures of credit terms, and the Fair Credit Billing Act, 15 U.S.C. §§ 1666 *et. seq.*, which provides for the correction of billing errors on credit accounts. The Commission also enforces over 30 rules governing specific industries and practices, eg, the Used Car Rule, 16 C.F.R. Part 455, which requires used car dealers to disclose warranty terms via a window sticker; the Franchise Rule, 16 C.F.R. Part 436, which requires the provision of information to prospective franchisees; and the Telemarketing Sales Rule, 16 C.F.R. Part 310, which defines and prohibits deceptive telemarketing practices and other abusive telemarketing practices.

5. The Commission held its first public workshop on online privacy in April 1995. In a series of hearings held in October and November 1995, the Commission examined the implications of globalization and technological innovation for competition issues and consumer protection issues, including privacy concerns. At a public workshop held in June 1996, the Commission examined Web site practices in the collection, use, and transfer of consumers' personal information; self-regulatory efforts and technological developments to enhance consumer privacy; consumer and business education efforts; the role of government in protecting online information privacy; and special issues raised by the online collection and use of information from and about children. The Commission held a second workshop in June 1997 to explore issues raised by individual reference services, as well as issues relating to unsolicited commercial e-mail, online privacy generally, and children's online privacy.

These efforts have served as a foundation for dialogue among members of the information industry and online business community, government representatives, privacy and consumer advocates, and experts in interactive technology. Further, the Commission and its staff have issued reports describing various privacy concerns in the electronic marketplace. *See, e.g., Individual Reference Services: A Federal Trade Commission Report to Congress* (December 1997); FTC Staff Report: *Public Workshop on Consumer Privacy on the Global Information Infrastructure* (December 1996); FTC Staff Report: *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace* (May 1996).

The Commission has also brought enforcement actions under Section 5 of the Federal Trade Commission Act to address deceptive online information practices. In 1998 the Commission announced its first Internet privacy case, in which GeoCities, operator of one of the most popular sites on the World Wide Web, agreed to settle Commission charges that it had misrepresented the purposes for which it was collecting personal identifying information from children and adults through its online membership application form and registration forms for children's activities on the GeoCities site. The settlement, which was made final in February 1999, prohibits GeoCities from misrepresenting the purposes for which it collects personal identifying information from or about consumers, including children. It also requires GeoCities to post a prominent privacy notice on its site, to establish a system to obtain parental consent before collecting personal information from children, and to offer individuals from whom it had previously collected personal information an opportunity to have that information deleted. *GeoCities*, Docket No C-3849 (Feb 12, 1999) (Final Decision and Order available at <http://www.ftc.gov/os/1999/9902/9823015d&o.htm>)

In its second Internet privacy case, the Commission recently announced for public comment a settlement with Liberty Financial Companies, Inc., operator of the Young Investor Web site. The Commission alleged, among other things, that the site falsely represented that personal information collected from children, including information about family finances, would be maintained anonymously. In fact, this information was maintained in identifiable form. The consent agreement would require Liberty Financial to post a privacy policy on its children's sites and obtain verifiable consent before collecting personal identifying information from children. *Liberty Financial*, Case No. 9823522 (proposed consent agreement available at <http://www.ftc.gov/os/1999/9905/1btyord.htm>.)

Since the fall of 1994, the Federal Trade Commission has brought 91 law enforcement actions against over 200 companies and individuals to halt fraud and deception on the Internet. The FTC has not only attacked traditional schemes that have moved online, like pyramid and credit repair schemes, but in addition, the FTC has brought suit against modem hijacking, fraudulent e-mail marketing, and other hi-tech schemes that take unique advantage of the Internet. The Commission pioneered the "Surf Day" concept and has searched the Net in tandem with law enforcement colleagues around the world, targeting specific problems and warning consumers and new entrepreneurs about what the law requires. The Commission has also posted "teaser pages" online, i.e., fake scam sites that give consumers education just when they are about to fall victim to an Internet ruse.

6. The Report is available on the Commission's Web site at <http://www.ftc.gov/reports/privacy3/index.htm>.

7. 1998 Report at 41.

8. Title XIII, Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, Pub L No 105-277, 112 Stat 2681, ____ (Oct. 21, 1998), *reprinted at* 144 Cong Rec H11240-42 (Oct. 19, 1998). The Act requires, inter alia, that operators of Web sites directed to children under 13 or who knowingly collect personal information from children under 13 on the Internet: (1) provide parents notice of their information practices; (2) obtain prior, verifiable parental consent for the collection, use, and/or disclosure of personal information from children (with certain limited exceptions); (3) upon request, provide a parent with the ability to review the personal information collected from his/her child; (4) provide a parent with the opportunity to prevent the further use of personal information that has already been collected, or the future collection of personal information from that child; (5) limit collection of personal information for a child's online participation in a game, prize offer, or other activity to information that is reasonably necessary for the activity; and (6) establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information collected.

9. 64 Fed Reg. 22750 (1999) (to be codified at 16 C.F.R. pt 312).

10. Commission testimony on *Consumer Privacy on the World Wide Web* before the House Subcommittee on Telecommunications, Trade and Consumer Protection, Committee on Commerce (July 21, 1998) (available at <http://www.ftc.gov/os/1998/9807/privac98.htm>). The Commission also presented a legislative model that Congress could consider in the event that then-nascent self-regulatory efforts did not result in widespread implementation of self-regulatory protections. *Id.* at 5-7.

11. A copy of the Report is attached as an appendix. The Report is available on the Commission's Web site at www.ftc.gov/reports/privacy99/index.html. In addition, the Commission testified on July 13, 1999 before the Subcommittee on Telecommunications, Trade, and Consumer Protection of the House Committee on Commerce on *Self-Regulation and Privacy Online* (www.ftc.gov/os/1999/9907/pt071399.htm). The Commission also presented testimony on July 21, 1999 before the Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Banking and Financial Services on *Financial Privacy, the Fair Credit Reporting Act*, and H.R. 10 (www.ftc.gov/os/1999/9907/ferahr10.htm). The Commission vote to issue that testimony and the Report was 3-1, with Commissioner Anthony concurring in part and dissenting in part Commissioner Anthony's statement and Commissioner Swindle's concurring statement were attached to the documents.

12. This aspect of the bill is consistent with the model recommended by the Commission in its July 21, 1998 testimony.

13. The report is available at <http://www.msb.edu/faculty/culnanm/gippshome.html> [hereinafter "GIPPS Report"]. The following analysis is based upon the Commission's review of the GIPPS Report itself; Commission staff did not have access to the underlying GIPPS data.

14. GIPPS Report, App. A at 5.

15. *Id.*

16. The GIPPS Report discusses findings on the information practices of 361 Web Sites drawn from a list of the 7,500 busiest servers on the World Wide Web. The list, a ranking of servers by number of unique visitors for the month of January 1999, was compiled by Media Metrix, a site traffic measurement company. As larger sites are more likely to have multiple servers, the largest sites on the Web had a greater chance of being selected for inclusion in the sample drawn for the GIPPS survey. See GIPPS Report, App. A at 2; App. B at 9 n.iii. The Commission's 1998 Comprehensive Sample was drawn at random from all U.S., ".com" sites in the Dun & Bradstreet Electronic Commerce Registry, with the exception of insurance industry sites. 1998 Report, App. A at 2. Unlike the Media Metrix list used in the GIPPS sample, the Dun & Bradstreet Registry does not rank sites on the basis of user traffic.

17. Online Privacy Alliance, *Privacy and the Top 100 Sites: A Report to the Federal Trade Commission* at 3, 8 (1999) (available at <http://www.msb.edu/faculty/culnanm/gippshome.html>). The following analysis is based upon the Commission's review of the OPA Study report itself; Commission staff did not have access to the underlying OPA Study data.

18. 1998 Report at 28.

19. Ninety-three percent of the sites in the GIPPS survey, GIPPS Report, App. A at 3, and 99% of the sites in the OPA Study, OPA Study at 3, 5, collect personal information from consumers.

20. The GIPPS results show that thirty-six sites in the sample (or 10%) posted at least one survey element, or disclosure, for each of the four substantive fair information practices. GIPPS Report at 10 and App. A at 12 (Table 8C). Thirty-two of these sites (or 89%) also posted contact information. *Id.* Georgetown University Professor Mary Culnan, author of the GIPPS Report, reports the number of sites posting disclosures for the four substantive fair information practice principles and for contact information in two additional ways: as a percentage of sites in the sample that collect at least one type of personal information (95%); and as a percentage of sites in the sample that both collect at least one type of personal information and post a disclosure (13.6%). GIPPS Report, App. A at 12 (Table 8C).

21. Twenty-two sites in the OPA Study (or 22%) posted at least one survey element, or disclosure, for each of the four substantive fair information practices. OPA Study at 9–10 and App. A at 10 (Table 6C). Nineteen of these sites (or 19%) also posted contact information. *Id.* Professor Culnan also reports the number of sites posting disclosures for the four substantive fair information practice principles in two additional ways: as a percentage of sites in the sample that collect at least one type of personal information (222%); and as a percentage of sites in the sample that both collect at least one type of personal information and post a disclosure (237%). OPA Study, App. A at 10 (Table 6C).

22. The Commission's 1998 Report discussed the fair information practice principles developed by government agencies in the United States, Canada, and Europe since 1973, when the United States Department of Health, Education, and Welfare released its seminal report on privacy protections in the age of data collection, *Records, Computers, and the Rights of Citizens*. 1998report at 7–11. In addition to the HEW Report, the major reports setting forth the core fair information practice principles are: The U.S. Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977); *Organization for Economic Cooperation and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980); *U.S. Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* (1995); *U.S. Dept of Commerce, Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (1995); *The European Union Directive on the Protection of Personal Data* (1995); and *the Canadian Standards Association, Model Code for the Protection of Personal Information: A National Standard of Canada* (1996). The 1998 Report identified the core principles of privacy protection common to these government reports, guidelines, and model codes: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress 1998 Report at 7–11.

The Notice/Awareness principle is the most fundamental: consumers must be given notice of a company's information practices before personal information is collected from them. The scope and content of the notice will vary with a company's substantive information practices, but the notice itself is essential. The other core principles have meaning only if a consumer has notice of an entity's information practices and his or her rights with respect thereto. *Id.* at 7.

The Choice/Consent principle requires that consumers be given options with respect to whether and how personal information collected from them may be used. Although choice in this context has been traditionally thought of as either "opt-in" (prior consent for use of information) or "opt-out" (limitation upon further use of information), *id.* at 9, interactive media hold the promise of making this paradigm obsolete through developments in technology. *Id.* The Access/Participation principle requires that consumers be given reasonable access to information collected about them and the ability to contest that data's accuracy and completeness. *Id.*

The Integrity/Security principle requires that companies take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use. *Id.* at 10. Finally, the effectiveness of the foregoing privacy protections is dependent upon implementation of the Enforcement/Redress principle, which requires governmental and/or self-regulatory mechanisms to impose sanctions for non-compliance with fair information practices. *Id.* at 10–11. The 1998 Report assessed existing self-regulatory efforts in light of these fair information practice principles.

23. Information about TRUSTe is taken from materials posted on TRUSTe's Web site, <http://www.TRUSTe.org>, and from public statements by TRUSTe staff. Several hundred additional companies have joined the TRUSTe program but are not yet fully licensed. See "TRUSTe Testifies Before House Judiciary Committee," May 27, 1999 (press release available at <http://www.TRUSTe.org/about/about—committee.html>).

24. Information about BBBOonline is taken from materials posted on the BBBOonline Web site, located at <http://www.bbbonline.com>, and from other public documents and statements by BBBOonline staff.

25. CPA WebTrust, the online privacy seal program created by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants, currently has 19 licensees (program description available at <http://www.cpawebtrust.org>). The Electronic Software Rating Board's ESRB Privacy Online program was launched on June 1, 1999 (description available at <http://www.esrb.org>).

MICROSOFT,
Washington, DC., July 30, 1999.

Hon. RICHARD H. BRYAN,
U.S. Senate,
Washington, DC.

Re: The Communications Subcommittee's July 27 Hearing on Privacy on the Internet

DEAR SENATOR BRYAN: This is to respond to a statement made by the America Online witness at the Subcommittee's July 27 hearing on "Privacy on the Internet." The statement was made in response to your question about AOL's current dispute with Microsoft and others in the Internet community over "instant messaging" services.

We understand that you asked AOL witness Jill Lesser whether her company's efforts to block the interoperation of AOL Instant Messenger with new instant messaging services such as our own—thereby closing off the AOL service from competing services—contradict AOL's argument that cable operators should open their new digital networks to competing internet service providers. The AOL witness defended here company's actions by alleging, among other things, that Microsoft had not spoken to AOL about our desire to foster interoperability in this area.

Ms. Lesser might not have had all of the facts at her disposal. As far back as late 1997, Microsoft and AOL personnel engaged in lengthy discussions about Microsoft's interest in working with AOL on new, interoperable instant messaging technologies. Those discussions did not bear fruit. Subsequently, Microsoft personnel participated in, and continue to participate in, an undertaking by the Internet Engineering task force to develop interoperability standards for instant messaging. IETF is one of the Internet's recognized standards bodies, and its actions are based on consensus among interested parties from the Internet community. With respect to instant messaging, we understand that AOL personnel had been invited on several occasions to participate in IETF deliberations on interoperability, but that the company had opted not to join.

Although the AOL misstatement does not relate to Internet privacy, we respectfully request that you ask for this letter to be inserted into the record of the hearing so that it accurately reflects what has transpired on this separate matter. Thank you.

Sincerely,

JACK KRUMHOLTZ, *Director,*
Federal Government Affairs Senior Corporate Attorney.

SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS

I. INTRODUCTION AND BACKGROUND

In June 1998 the Federal Trade Commission issued *Privacy Online: A Report to Congress* ("1998 Report"), an examination of the information practices of commercial sites on the World Wide Web and of industry's efforts to implement self-regulatory programs to protect consumers' online privacy.¹ Based in part on its extensive survey of over 1400 commercial Web sites, the Commission concluded that effective self-regulation had not yet taken hold.² In both the 1998 Report and in subsequent testimony before Congress, the Commission raised concerns about protecting the privacy of children's personal information online and recommended that Congress pass legislation to address these concerns.³ In its testimony, the Commission also raised concerns about the progress of industry self-regulation, but noted that industry leaders had indicated their commitment to work toward self-regulatory solutions. Accordingly, the Commission did not recommend legislative action in the area of online

privacy for consumers generally, and instead urged industry to focus on developing and implementing broad-based and effective self-regulatory programs.⁴

In the ensuing year, there have been important developments both in the growth of the Internet as a commercial marketplace and in consumers' and industry's responses to the privacy issues posed by the online collection of personal information. The Commission has examined these developments and now presents its views on the progress made in self-regulation since last June, as well as its plans to encourage industry's full implementation of online privacy protections.

A. *The Growth of Electronic Commerce*

Commerce on the World Wide Web is booming. The United States Department of Commerce recently announced that online sales tripled from approximately \$3 billion in 1997 to approximately \$9 billion in 1998.⁵ Online revenues of North American retailers in the first half of 1998 were approximately \$4.4 billion.⁶ Online advertising revenues have grown from \$906.5 million in 1996 to \$1.92 billion in 1998.⁷ In 1998, revenues for Internet advertising exceeded those for advertising on outdoor billboards.⁸ It is estimated that almost 80 million adults in the United States are using the Internet.⁹ They are finding a vast array of products, services, and information in a marketplace that has experienced exponential growth since its beginnings only a few years ago.

The Web is also a rich source of information *about* online consumers. Web sites collect much personal information both explicitly, through registration pages, survey forms, order forms, and online contests, and by using software in ways that are not obvious to online consumers. Through "cookies" and tracking software, Web site owners are able to follow consumers' online activities and gather information about their personal interests and preferences. These data have proved extremely valuable to online companies because they not only enable merchants to target market products and services that are increasingly tailored to their visitors' interests, but also permit companies to boost their revenues by selling advertising space on their Web sites.¹⁰ In fact, an entire industry has emerged to market a variety of software products designed to assist Web sites in collecting and analyzing visitor data and in serving targeted advertising.¹¹

B. *Consumer Privacy Concerns*

Notwithstanding the substantial benefits that consumers may derive from using the Internet, consumers still care deeply about the privacy of their personal information in the online marketplace. Eighty-seven percent of U.S. respondents in a recent survey of experienced Internet users stated that they were somewhat or very concerned about threats to their privacy online.¹² Seventy percent of the respondents in a recent national survey conducted for the National Consumers League reported that they were uncomfortable providing personal information to businesses online.¹³ Consumers are particularly concerned about potential transfers to third parties of the personal information they have given to online businesses.¹⁴ It is not surprising that only about one-quarter of Internet users go beyond merely browsing for information to actually purchasing goods and services online.¹⁵

II. THE COMMISSION'S APPROACH TO ONLINE PRIVACY

For almost as long as there has been an online marketplace, the Commission has been deeply involved in addressing online privacy issues.¹⁶ The Commission's goal has been to understand this new marketplace and its information practices, to assess the impact of these practices on consumers, and to encourage and facilitate effective self-regulation as the preferred approach to protecting consumer privacy online. The Commission's efforts have been based on the belief that greater protection of personal privacy on the Web will not only benefit consumers, but also benefit industry by increasing consumer confidence and ultimately their participation in the online marketplace.

The Commission's 1998 Report discussed the fair information practice principles developed by government agencies in the United States, Canada, and Europe since 1973, when the United States Department of Health, Education, and Welfare released its seminal report on privacy protections in the age of data collection, *Records, Computers, and the Rights of Citizens*.¹⁷ The 1998 Report identified the core principles of privacy protection common to the government reports, guidelines, and model codes that have emerged since 1973: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.¹⁸

The Notice/Awareness principle is the most fundamental: consumers must be given notice of a company's information practices before personal information is collected from them. The scope and content of the notice will vary with a company's

substantive information practices, but the notice itself is essential. The other core principles have meaning only if a consumer has notice of an entity's information practices and his or her rights with respect thereto.

The other core principles are briefly summarized here. The Choice/Consent principle requires that consumers be given options with respect to whether and how personal information collected from them may be used.¹⁹ The Access/Participation principle requires that consumers be given reasonable access to information collected about them and the ability to contest that data's accuracy and completeness.²⁰ The Integrity/Security principle requires that companies take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use.²¹ Finally, the effectiveness of the foregoing privacy protections is dependent upon implementation of the Enforcement/Redress principle, which requires governmental and/or self-regulatory mechanisms to impose sanctions for noncompliance with fair information practices.²²

The 1998 Report assessed existing self-regulatory efforts in light of these fair information practice principles and set out the findings of the Commission's extensive survey of commercial Web sites' information practices. The survey found that, although the vast majority of sites collected personal information from consumers—92% in the sample representing all U.S.-based commercial sites likely to be of interest to consumers—only 14% posted any disclosure regarding their information practices, and only 2% posted a comprehensive privacy policy.²³ The results of the Commission's census of the busiest sites on the World Wide Web were more positive: while 97% collected personal information, 71% posted a disclosure and 44% posted a comprehensive privacy policy.²⁴ The Commission's survey of sites directed to children revealed that 89% collected personal information from children, 24% posted privacy policies and only 1% required parental consent prior to the collection or disclosure of children's information.²⁵

The 1998 Report concluded that an effective self-regulatory system had yet to emerge and that additional incentives were required in order to ensure that consumer privacy would be protected. Noting its particular concern about the vulnerability of children, the Commission recommended that Congress adopt legislation setting forth standards for the online collection of information from children. Furthermore, in Congressional testimony last July, the Commission deferred judgment on the need for legislation to protect the online privacy of adult consumers, but presented a legislative model that Congress could consider if industry failed to develop and implement effective self-regulatory measures.²⁶

III. CONGRESSIONAL RESPONSE

On October 21, 1998, the President signed into law the Children's Online Privacy Protection Act of 1998 ("COPPA").²⁷ The Act, passed by Congress just four months after the Commission's 1998 Report, requires that operators of Web sites directed to children under 13 or who knowingly collect personal information from children under 13 on the Internet: (1) provide parents notice of their information practices; (2) obtain prior, verifiable parental consent for the collection, use, and/or disclosure of personal information from children (with certain limited exceptions); (3) upon request, provide a parent with the ability to review the personal information collected from his/her child; (4) provide a parent with the opportunity to prevent the further use of personal information that has already been collected, or the future collection of personal information from that child; (5) limit collection of personal information for a child's online participation in a game, prize offer, or other activity to information that is reasonably necessary for the activity; and (6) establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information collected.²⁸ The Act directs the Commission to adopt within one year regulations implementing these requirements.²⁹

On April 20, 1999, the Commission issued a proposed Children's Online Privacy Protection Rule and is now in the midst of this rulemaking effort.³⁰ The proposed rule requires Web site operators to post prominent links on their Web sites to a notice of how they collect and use personal information from children under the age of 13, and sets out, among other things, standards for complying with the Act's notice, parental consent, and access requirements.³¹ As required by the COPPA, the proposed rule also includes a safe harbor provision under which industry groups or others may seek Commission approval for self-regulatory guidelines. Web site operators who participate in such approved programs may be subject to the review and disciplinary procedures provided in those guidelines in lieu of formal Commission investigation and law enforcement.³² The safe harbor would serve both as an incentive for industry self-regulation, and as a means of ensuring that the Act's protections are implemented in a manner sensitive to industry-specific concerns and devel-

opments in technology. Commission staff is reviewing comments on the proposed rule and will hold a public workshop this month to solicit further discussion and comment on the issue of verifiable parental consent. The Commission will issue a final rule this fall.

IV. THE STATE OF ONLINE PRIVACY SELF-REGULATION TODAY

As noted in the Commission's 1998 Report, self-regulation is the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology. During the past year the Commission has been monitoring self-regulatory initiatives to address the privacy concerns of online consumers. In some areas, there has been much progress. The results of two new surveys of commercial Web sites suggest that online businesses are providing significantly more notice of their information practices than they were last year. In addition, several significant and promising self-regulatory programs, including privacy seal programs, are underway.

There are also major challenges for self-regulation. The new survey results show that, despite the laudable efforts of industry leaders, the vast majority of even the busiest Web sites have not implemented all four substantive fair information practice principles of Notice/Awareness, Choice/Consent, Access/Participation, and Security/Integrity. In addition, the seal programs discussed below currently encompass only a handful of all Web sites. Thus, it is too early to judge how effective these programs will ultimately be in serving as enforcement mechanisms to protect consumers' online privacy.

The Commission believes that there are additional steps that it can take, together with industry, and consumer and privacy groups, to build upon the progress in self-regulation to date and to work toward full implementation of effective online privacy protections. Some recent developments and plans for future work to achieve this goal are discussed below.

A. Recent Assessments of Web Sites' Compliance With Fair Information Practice Principles

Professor Mary Culnan of the McDonough School of Business at Georgetown University recently announced the results of two industry-funded surveys of commercial Web sites, conducted during the week of March 8, 1999. The Georgetown Internet Privacy Policy Survey ("GIPPS")³³ reports findings on the information practices of 361 Web sites drawn from a list of the 7,500 busiest servers on the World Wide Web.³⁴ Ninety-three percent of the sites in this survey collect personal information from consumers, and 66% post at least one disclosure about their information practices.³⁵ Forty-four percent of these sites post privacy policy notices.³⁶ Although differences in sampling methodology prevent direct comparisons between the GIPPS findings and the Commission's 1998 results,³⁷ the GIPPS Report does demonstrate the real progress industry has made in giving consumers notice of at least some information practices. On the other hand, only 10% of the sites in the GIPPS sample are implementing all four substantive fair information practice principles of Notice/Awareness, Choice/Consent, Access/ Participation, and Security/Integrity.³⁸ The GIPPS Report findings discussed above are summarized in Figure 1.

Professor Culnan also conducted a census of the top 100 Web sites commissioned by the Online Privacy Alliance, a coalition of more than eighty online companies and trade associations that formed early in 1998 to encourage self-regulation in this area ("OPA Study").³⁹ As is true of the GIPPS sample, nearly all (99%) of the sites in the OPA Study collect personal information from consumers. Ninety-three percent of these sites provide at least one disclosure about their information practices, while 81% of these sites post privacy policy notices.⁴⁰ This represents continued progress since last year, when 71% of the sites in the Commission's 1998 "Most Popular" sample posted an information practice disclosure.⁴¹ Only 22% of the sites in the OPA study address all four of the substantive fair information practice principles of Notice/Awareness, Choice/Consent, Access/Participation and Security/Integrity, however.⁴² These OPA Study findings are summarized in Figure 1.

Figure 1

	1999 GIPPS Report	1999 OPA Study
Number of sites in sample	361	100
Number of sites collecting personal information	337	99
Percent of sites in sample collecting personal information	93%	99%
Number of sites posting any privacy disclosure	238	93

Figure 1—Continued

	1999 GIPPS Report	1999 OPA Study
Percent of sites in sample posting any privacy disclosure	66%	93%
Number of sites posting a privacy policy notice	157	81
Percent of sites in sample posting a privacy policy notice	44%	81%
Number of sites posting a disclosure for all four substantive fair information practice principles	36	22
Percent of sites in sample posting a disclosure for all four substantive fair information practice principles	10%	22%

The GIPPS and OPA Study results suggest that the majority of the more frequently-visited Web sites are implementing the basic Notice/Awareness principle by disclosing at least some of their information practices. The findings also indicate, however, that only a relatively small percentage of these sites is disclosing information practices that address all four substantive fair information practice principles. Both studies indicate that there has been real progress since the Commission issued its 1998 Report. Nevertheless, the low percentage of sites in both studies that address all four substantive fair information practice principles demonstrates that further improvement is required to effectively protect consumers' online privacy.

B. The Online Privacy Alliance⁴³

On June 22, 1998, the Online Privacy Alliance (OPA), a coalition of industry groups, announced its Online Privacy Guidelines, which apply to individually identifiable information collected online from consumers.⁴⁴ Pursuant to these guidelines, OPA members agree to adopt and implement a posted privacy policy that provides comprehensive notice of their information practices. The notice includes a statement of what information is being collected from consumers and how it is being used; whether the information will be disclosed to third parties; consumers' choices regarding the collection, use and distribution of the information; data security measures; and the steps taken to ensure data quality and access to information. The OPA Guidelines also include provisions on choice, feasible consumer access to identifiable information, and data security, and call for self-enforcement mechanisms, such as online seal programs, that provide consumers with redress.

The OPA Guidelines have been used by the leading privacy seal programs, which have adapted them to fit their own program requirements. Unlike the seal programs, however, the OPA does not monitor members' compliance or provide sanctions for noncompliance. The central focus of OPA's efforts since release of its Guidelines has been business education to promote widespread adoption of online privacy policies.

C. Seal Programs

An encouraging development in the private sector's efforts toward self-regulation is the emergence of online seal programs. These programs require their licensees to abide by codes of online information practices and to submit to various types of compliance monitoring in order to display a privacy seal on their Web sites. Seal programs offer an easy way for consumers to identify Web sites that follow specified information practice principles, and for online businesses to demonstrate compliance with those principles.

1. TRUSTe⁴⁵

TRUSTe, an independent, non-profit organization founded by the CommerceNet Consortium and the Electronic Frontier Foundation, was launched nearly two years ago, on June 10, 1997. The first online privacy seal program, TRUSTe currently has more than 500 licensees representing a variety of industries.⁴⁶ Since December 1998, TRUSTe's license agreement,⁴⁷ which governs licensees' collection and use of "personally identifiable information,"⁴⁸ has taken a more comprehensive approach to privacy by requiring licensees to follow standards for notice, choice, access and security based upon the OPA Guidelines. The license agreement also requires licensees to submit to monitoring and oversight by TRUSTe, as well as a complaint resolution procedure.

The TRUSTe program includes third-party monitoring and periodic reviews of licensees' information practices to ensure compliance with program requirements. These reviews include "Web Site reviews," in which TRUSTe examines and monitors changes in licensees' privacy statements and tracks unique identifiers in licensees' databases (a practice known as "seeding") to determine whether consumers' requests to be removed from those databases are being honored; and "On-Site reviews" in

which a third-party auditing firm can be called in, should TRUSTe have reason to believe that a licensee is not in compliance with the terms of the license agreement. Licensees must provide consumers with a way to submit concerns regarding their information practices, and agree to respond to all reasonable inquiries within five days. TRUSTe also plays a part in resolving consumer complaints. TRUSTe provides for public reporting of complaints, and, in appropriate circumstances, will refer complaints to the Commission.

2. *BBBOnline Privacy Seal Program*⁴⁹

BBBOnline, a subsidiary of the Council of Better Business Bureaus, launched its privacy seal program for online businesses on March 17, 1999. Forty-two sites currently post BBBOnline seals, and the program has received more than 300 applications. In order to be awarded the BBBOnline Privacy Seal, applicants must post a privacy policy that comports with the program's information practice principles,⁵⁰ complete a "Compliance Assessment Questionnaire," and must agree to participate in a consumer dispute resolution system and to submit to monitoring and review by BBBOnline.⁵¹

The BBBOnline Privacy Seal Program covers "individually identifiable information,"⁵² as well as "prospect information," which is identifying, retrievable information that is collected by the company's Web site from one individual about another.⁵³ The BBBOnline Privacy Seal Program's consumer complaint resolution procedure is bolstered by several compliance incentives, including public reporting of decisions, and suspension or revocation of the BBBOnline seal, or referral to federal agencies, as sanctions for noncompliance. BBBOnline has committed to adopting a third-party verification system, although this aspect of the program has not yet been implemented. The Commission looks forward to assessing BBBOnline's enforcement mechanisms when they are fully in place.

3. *Other Seal Programs*

Several other seal programs have been developed or are under development. One is CPA WebTrust, created by the American Institute of Certified Public Accountants ("AICPA") and the Canadian Institute of Chartered Accountants and announced in September 1997.⁵⁴ The CPA WebTrust program, which licenses the CPA WebTrust seal to qualifying certified public accountants, requires participating Web sites to disclose and adhere to stated business practices, maintain effective controls over the security and integrity of transactions, and to maintain effective controls to protect private customer information. Web sites are awarded the CPA WebTrust seal by certified public accountants who conduct quarterly audits to ensure compliance with the program's standards.

Although primarily intended to provide assurance for consumers that a site displaying the seal is a legitimate business that will process transactions and protect sensitive information like credit card numbers, CPA WebTrust also has a privacy component. The information practice requirements in the latest version of the program, introduced in May 1999, conform to the OPA Guidelines. Currently, 19 Web sites have been awarded the CPA WebTrust seal.

Industry sector-specific programs are also beginning to emerge. For example, in October 1998 the Interactive Digital Software Association ("IDSA") adopted its own fair information practice guidelines for its members' Web sites.⁵⁵ In addition, on June 1, 1999, the Entertainment Software Rating Board ("ESRB"), an independent rating system for entertainment software and interactive games established by IDSA in 1994, launched ESRB Privacy Online.⁵⁶ This online seal program requires participants to adhere to information practice standards that parallel the IDSA guidelines.⁵⁷ The program monitors compliance through a verification system that includes unannounced audits and seeding. The program also includes a consumer online hotline for reporting privacy violations and alternative dispute resolution services to resolve consumer complaints.

V. CONCLUSION

The self-regulatory initiatives described above, including the guidelines adopted by the OPA and the seal programs, reflect industry leaders' substantial effort and commitment to information practices. They should be commended for these efforts. Enforcement mechanisms that go beyond self-assessment are also gradually being implemented by the seal Web programs. Only a small minority of commercial Web sites, however, have joined these programs to date. Similarly, although the results of the GIPPS and OPA studies show that many online companies now understand the business case for protecting consumer privacy, they also show that the implementation of fair information practices is not widespread among commercial Web sites.

Based on these facts, the Commission believes that legislation to address online privacy is not appropriate at this time. We also believe that industry faces some substantial challenges. Specifically, the present challenge is to educate those companies which still do not understand the importance of consumer privacy and to create incentives for further progress toward effective, widespread implementation.

First, industry groups must continue to encourage widespread adoption of fair information practices. Companies like IBM, Microsoft and Disney, which have recently announced, among other things, that they will forgo advertising on sites that do not adhere to fair information practices are to be commended for their efforts, which we hope will be emulated by their colleagues. These types of business-based initiatives are critical to making self-regulation meaningful because they can extend the reach of privacy protection to small and medium-sized businesses where there is great potential for e-commerce growth.

Second, industry should focus its attention on the substance of Web site information practices, ensuring that companies adhere to the core privacy principles discussed earlier. It may also be appropriate, at some point in the future, for the FTC to examine the online privacy seal programs and report to Congress on whether these programs provide effective privacy protections for consumers.

Finally, industry must work together with government and consumer groups to educate consumers about privacy protection on the Internet. The ultimate goal of such efforts, together with effective self-regulation, will be heightened consumer acceptance and confidence. Industry should also redouble its efforts to develop effective technology to provide consumers with tools they can use to safeguard their own privacy online.

The Commission has developed an agenda to address online privacy issues throughout the coming year as a way of encouraging and, ultimately, assessing further progress in self regulation to protect consumer online privacy:

- The Commission will hold a public workshop on “online profiling,” the practice of aggregating information about consumers’ preferences and interests gathered primarily by tracking their movements online, and, in some cases, combining this information with personal information collected directly from consumers or contained in other databases. The workshop, jointly sponsored by the U.S. Department of Commerce, will examine online advertising firms’ use of cookies and other tracking technologies to create targeted, user profile-based advertising campaigns.

- The Commission will hold a public workshop on the privacy implications of electronic identifiers that enhance Web sites’ ability to track consumers’ online behavior.

- In keeping with its history of fostering dialogue on online privacy issues among all stakeholders, the Commission will convene task forces of industry representatives and privacy and consumer advocates to develop strategies for furthering the implementation of fair information practices in the online environment.

One task force will focus upon understanding the costs and benefits of implementing fair information practices online, with particular emphasis on defining the parameters of the principles of consumer access to data and adequate security.

A second task force will address how incentives can be created to encourage the development of privacy-enhancing technologies, such as the World Wide Web Consortium’s Platform for Privacy Preferences (P3P).

- The Commission, in partnership with the U.S. Department of Commerce, will promote private sector business education initiatives designed to encourage new online entrepreneurs engaged in commerce on the Web to adopt fair information practices.

- Finally, the Commission believes it is important to continue to monitor the progress of self-regulation, to determine whether the self-regulatory programs discussed in this report fulfill their promise. To that end, the Commission will conduct an online survey to reassess progress in Web sites’ implementation of fair information practices, and will report its findings to Congress.

In undertaking these efforts, the Commission will be better able to assess industry progress in meeting its self-regulatory responsibilities, while fostering the implementation of effective protections for online privacy in a manner that promotes a flourishing electronic marketplace.

ENDNOTES

1. The Report is available on the Commission’s Web site at <http://www.ftc.gov/reports/privacy3/index.htm>.

2. 1998 Report at 41.

3. 1998 Report at 42; Commission testimony on Consumer Privacy on the World Wide Web before the House Subcommittee on Telecommunications, Trade and Consumer Protection, Committee on Commerce (July 21, 1998) at 4–5 [hereinafter “1998 Privacy Testimony”] (available at <http://www.ftc.gov/os/1998/9807/privac98.htm>).

4. 1998 Privacy Testimony at 4. The Commission also presented a legislative model that Congress could consider in the event that then-nascent self-regulatory efforts did not result in widespread implementation of self-regulatory protections. *Id.* at 5–7.

5. Remarks of Secretary of Commerce William M. Daley, Feb. 5, 1999 (text available at <http://204.193.246.62/public.nsf/docs/commerce-ftc-online-shopping-briefing>).

6. The Boston Consulting Group, *The State of Online Retailing* 7 and App. A (Nov. 1998).

7. Internet Advertising Bureau, *Advertising Revenue Report* (May 1999) (major findings available at <http://www.iab.net/news/content/1998results.html>).

8. *Id.*

9. Intelliquest, Inc., *Worldwide Internet/Online Tracking Service 4th Quarter 1998 Report* (results available at <http://www.intelliquest.com>).

10. See Forrester Research, Inc., *Media & Technology Strategies: Making Users Pay* at 4–6 (1998).

11. See, e.g., Rivka Tadjer, “Following the Patron Path,” *ZD Internet Magazine*, Dec. 1997, at 95; Thomas E. Weber, “Software Lets Marketers Target Web Ads,” *Wall St. J.*, Apr. 21, 1997, at B1.

12. Lorrrie Faith Cranor, et al., *Beyond Concern: Understanding Net Users’ Attitudes About Online Privacy* at 5 (1999) [hereinafter “AT&T Study”] (available at <http://www.research.att.com/projects/privacystudy>).

13. Louis Harris & Associates, Inc., *National Consumers League: Consumers and the 21st Century* at 4 (1999).

14. AT&T Study at 2, 10.

15. Intelliquest, Inc., *Worldwide Internet/Online Tracking Service 1st Quarter 1999 Report* (findings summarized at <http://www.intelliquest.com/press/release78.asp>) (28%); Louis Harris & Associates, Inc. and Alan F. Westin, *E-Commerce & Privacy: What Net Users Want* at 1 (1998) (23%).

16. The Commission held its first public workshop on privacy in April 1995. In a series of hearings held in October and November 1995, the Commission examined the implications of globalization and technological innovation for competition issues and consumer protection issues, including privacy concerns. At a public workshop held in June 1996, the Commission examined Web site practices in the collection, use, and transfer of consumers’ personal information; self-regulatory efforts and technological developments to enhance consumer privacy; consumer and business education efforts; the role of government in protecting online information privacy; and special issues raised by the online collection and use of information from and about children. The Commission held a second workshop in June 1997 to explore issues raised by individual reference services, as well as issues relating to unsolicited commercial e-mail, online privacy generally, and children’s online privacy.

These efforts have served as a foundation for dialogue among members of the information industry and online business community, government representatives, privacy and consumer advocates, and experts in interactive technology. Further, the Commission and its staff have issued reports describing various privacy concerns in the electronic marketplace. See, e.g., *Individual Reference Services: A Federal Trade Commission Report to Congress (December 1997)*; *FTC Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure (December 1996)*; *FTC Staff Report: Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace (May 1996)*.

The Commission has also brought enforcement actions under Section 5 of the Federal Trade Commission Act to address deceptive online information practices. In 1998 the Commission announced its first Internet privacy case, in which GeoCities, operator of one of the most popular sites on the World Wide Web, agreed to settle Commission charges that it had misrepresented the purposes for which it was collecting personal identifying information from children and adults through its online membership application form and registration forms for children’s activities on the GeoCities site. The settlement, which was made final in February 1999, prohibits GeoCities from misrepresenting the purposes for which it collects personal identifying information from or about consumers, including children. It also requires GeoCities to post a prominent privacy notice on its site, to establish a system to obtain parental consent before collecting personal information from children, and to offer individuals from whom it had previously collected personal information an opportunity to have that information deleted. GeoCities, Docket No. C–3849 (Feb. 12,

1999) (Final Decision and Order available at <http://www.ftc.gov/os/1999/9902/9823015d&o.htm>).

In its second Internet privacy case, the Commission recently announced for public comment a settlement with Liberty Financial Companies, Inc., operator of the Young Investor Web site. The Commission alleged, among other things, that the site falsely represented that personal information collected from children, including information about family finances, would be maintained anonymously. In fact, this information was maintained in identifiable form. The consent agreement would require Liberty Financial to post a privacy policy on its children's sites and obtain verifiable consent before collecting personal identifying information from children. *Liberty Financial*, Case No. 9823522 (proposed consent agreement available at <http://www.ftc.gov/os/1999/9905/1btyord.htm>).

17. 1998 Report at 7–11. In addition to the HEW Report, the major reports setting forth the core fair information practice principles are: The U.S. Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977); *Organization for Economic Cooperation and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980); *U.S. Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* (1995); *U.S. Dept. of Commerce, Privacy and the NU: Safeguarding Telecommunications-Related Personal Information* (1995); *The European Union Directive on the Protection of Personal Data* (1995); and *the Canadian Standards Association, Model Code for the Protection of Personal Information: A National Standard of Canada* (1996).

18. 1998 Report at 7–11.

19. Although choice in this context has been traditionally thought of as either “opt-in” (prior consent for use of information) or “opt-out” (limitation upon further use of information), *id.* at 9, interactive media hold the promise of making this paradigm obsolete through developments in technology. *Id.*

20. *Id.* at 9.

21. *Id.* at 10.

22. *Id.* at 10–11.

23. *Id.* at 23, 27.

24. *Id.* at 24, 28.

25. *Id.* at 31, 35, 37.

26. 1998 Privacy Testimony at 5–7.

27. Title XIII, Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, Pub. L.105–277, 112 Stat. 2681, ____ (October 21, 1998), reprinted at 144 Cong. Rec. H11240–42 (Oct. 19, 1998). The goals of the Act are: (1) to enhance parental involvement in a child's online activities in order to protect the privacy of children in the online environment; (2) to help protect the safety of children in online fora such as chat rooms, home pages, and pen-pal services in which children may make public postings of identifying information; (3) to maintain the security of children's personal information collected online; and (4) to limit the collection of personal information from children without parental consent. 144 Cong. Rec. S12741 (Oct. 7, 1998) (Statement of Sen. Bryan).

28. Title XIII, Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, Pub. L.105–277, 112 Stat. 2681, ____ (October 21, 1998), reprinted at 144 Cong. Rec. H11240–42 (Oct. 19, 1998).

29. *Id.*

30. 64 Fed. Reg. 22750 (1999) (to be codified at 16 C.F.R. pt. 312).

31. *Id.* at 22753–58 (Proposed Rule §§ 312.4–312.6).

32. *Id.* at 22759–60 (Proposed Rule § 312.10).

33. The report is available at <http://www.msb.edu/faculty/culnanm/gippshome.html> [hereinafter “GIPPS Report”]. The following analysis is based upon the Commission's review of the GIPPS Report itself; Commission staff did not have access to the underlying GIPPS data.

34. GIPPS Report at 1; App. B at 4. The list, a ranking of servers by number of unique visitors for the month of January 1999, was compiled by Media Metrix, a site traffic measurement company. As larger sites are more likely to have multiple servers, the largest sites on the Web had a greater chance of being selected for inclusion in the sample drawn for this survey. See GIPPS Report, App. A at 1; App. B at 9 n.iii.

35. GIPPS Report, App. A at 3, 5.

36. GIPPS Report, App. A at 5.

37. The Commission's 1998 Comprehensive Sample was drawn at random from all U.S., “.com” sites in the Dun & Bradstreet Electronic Commerce Registry, with the exception of insurance industry sites. 1998 Report, App. A at 2. Unlike the Media

Metrix list used in the GIPPS sample, the Dun & Bradstreet Registry does not rank sites on the basis of user traffic.

38. The GIPPS results show that thirty-six sites in the sample (or 10%) posted at least one survey element, or disclosure, for each of the four substantive fair information practices. GIPPS Report at 10. Thirty-two of these sites (or 8.9%) also posted contact information. *Id.* and App. A at 12. Professor Culnan also reports the number of sites posting disclosures for the four substantive fair information practice principles and for contact information in two additional ways: as a percentage of sites in the sample that collect at least one type of personal information (9.5%); and as a percentage of sites in the sample that both collect at least one type of personal information and post a disclosure (13.6%). GIPPS Report, App. A at 12 (Table 8C).

39. Online Privacy Alliance, *Privacy and the Top 100 Sites: A Report to the Federal Trade Commission* (1999) (available at <http://www.msb.edu/faculty/culnanm/gippshome.html>). The following analysis is based upon the Commission's review of the OPA Study report itself; Commission staff did not have access to the underlying OPA Study data.

40. OPA Study at 3, 5, and 8.

41. 1998 Report at 28.

42. Twenty-two sites in the OPA Study (or 22%) posted at least one survey element, or disclosure, for each of the four substantive fair information practices. OPA Study at 9–10 and App. A at 10 (Table 6C). Nineteen of these sites (or 19%) also posted contact information. *Id.* Professor Culnan also reports the number of sites posting disclosures for the four substantive fair information practice principles in two additional ways: as a percentage of sites in the sample that collect at least one type of personal information (22.2%); and as a percentage of sites in the sample that both collect at least one type of personal information and post a disclosure (23.7%). OPA Study, App. A at 10 (Table 6C).

43. The information included in this section is drawn from the OPA Web site (<http://www.privacyalliance.org>) and OPA members' testimony before the Senate Judiciary Committee's Hearing on Privacy in the Digital Age: Discussion of Issues Surrounding the Internet on April 21, 1999. The testimony is available on the OPA Web site, and at <http://www.senate.gov/judiciary/42199kb.htm>.

44. The Guidelines are available at <http://www.privacyalliance.org/resources/ppguidelines.shtml>.

45. The information in this section is taken from materials posted on TRUSTe's Web site, <http://www.TRUSTe.org>, and from public statements by TRUSTe staff.

46. Several hundred additional companies have joined the TRUSTe program but are not yet fully licensed. See "*TRUSTe Testifies Before House Judiciary Committee*," May 27, 1999 (press release available at <http://www.TRUSTe.org/about/about-committee.html>).

47. Not all of TRUSTe's current licensees are subject to the latest version of the license agreement.

48. "Personally identifiable information" is defined as any information that can be used to identify, contact, or locate a person, including information that may be linked with identifiable information from other sources, or from which other personally identifiable information can easily be derived.

49. The information in this section is taken from materials posted on the BBBOnline Web site, located at <http://www.bbbonline.com>, and from other public documents and statements by BBBOnline staff.

50. The BBBOnline Privacy Seal Program establishes requirements for notice, choice, access, and security. Comprehensive notice disclosures are required. Consumers must be allowed to prohibit unrelated uses of individually identifiable information not disclosed in the site's privacy policy and disclosure to third parties for marketing purposes. Consumers must also be permitted access to information about them to correct inaccuracies.

51. License fees to display the BBBOnline Privacy logo are determined by a sliding scale according to the participant's revenues. Currently, the annual license fee ranges from \$150 for companies with under \$1 million in sales, to \$3,000 for companies with sales over \$2 billion.

52. "Individually identifiable information" is defined as information that (1) can be used to identify an individual, (2) is elicited by the company's Web site through active or passive means from the individual, and (3) is retrievable by the company in the ordinary course of business.

53. "Prospect information" would be collected when, for example, a visitor to a site orders a gift for another person and supplies that person's mailing address.

It is not clear whether demographic information about a consumer that is collected at a site and tied to an identifier is covered by the BBBOnline program, although licensees are required to provide notice if they merge or enhance individ-

ually identifiable information with data from third parties for the purposes of marketing products or services to the consumer.

54. Information about CPA WebTrust is available at <http://www.cpawebtrust.org>.

55. *Privacy in the Digital Age: Discussion of Issues Surrounding the Internet*, before the Senate Judiciary Comm., 106th Cong., April 21, 1999 (prepared statement of Gregory Fischbach).

56. Information regarding the ESRB privacy seal program is available at <http://www.esrb.org>.

57. The program guidelines include standards for notice and disclosure; choice; limiting data collection and retention; data integrity/security; data access; and enforcement and accountability.

Senator BURNS. Thank you, Mr. Chairman. We have been joined on the committee this morning by Senator Wyden and Senator DORGAN.

Senator Wyden, do you have a statement or would you like to submit a statement?

**STATEMENT OF HON. RON WYDEN, U.S. SENATOR
FROM OREGON**

Senator WYDEN. Mr. Chairman, I would like to make a statement, but I will be very brief.

This is an excellent panel. Is that acceptable at this point?

Senator BURNS. That is acceptable.

Senator WYDEN. Thank you, Mr. Chairman. Let me begin by saying how much I appreciate working with you in developing S. 809. I think it is a balanced bill, and I have been pleased to work with you. In going forward with this bipartisan effort that you and I have launched, Mr. Chairman, I want to make it clear that first I believe in the power of free markets.

I think I showed with the Internet Tax Freedom Act, with the Y2K liability legislation, with what we have done in encryption that I feel strongly about the potential of the medium, but the reason that I want us to pass S. 809 is that I think it would be a great mistake for this country to essentially sit idly by and wait for an *Exon Valdez* style invasion of privacy before action is taken, and that is really what this legislation is all about.

Third, what is most telling to me is what the Nation's CEOs are saying about this issue in a recent survey by CEO Magazine. Sixty percent of the chief information officers in this country were unwilling to give personal information about themselves on line. I think if anything is telling about the need for a thoughtful, balanced bill, it is what the Nation's CEOs and their chief information officers are saying about the importance of this legislation.

Finally, the last point I would make is that the folks that are working for self-regulation, the many companies that have hired some of the most talented lobbyists in the Nation to fight privacy regulation, are not the companies that the United States Senate ought to be worried about. Those are the companies that have again and again reflected responsible corporate efforts to try to deal with these issues, and it is the bad actors that S. 809 is trying to target, not the companies that have formed this coalition, not the companies we work with on Internet, tax freedom, or encryption, or Y2K liability. I am very hopeful we can go forward with this legislation.

The last point I would make is a comment in response to what Bob Pitofsky said, and he as always has given very helpful testi-

mony. What we are trying to do in S. 809 is address your point with respect to making sure that this law is not outdated by the time it goes into effect. Principles like opting out and understandable disclosure requirements are the kinds of things that have stood the test of time at the Federal Trade Commission, and it is those kinds of principles that we want to use for the foundation of privacy policy, and speak to the important point you are making about making sure that the Congress does not do something foolish that is essentially outdated by the time it becomes law. I thank you for the chance to make that statement.

Senator BURNS. Thank you very much, Senator, and I appreciate working with you on this piece of legislation also.

Senator Dorgan, do you have a statement?

STATEMENT OF HON. BYRON L. DORGAN, U.S. SENATOR FROM NORTH DAKOTA

Senator DORGAN. Mr. Chairman, I will submit a statement for the record.

I did want to thank you for the hearing and indicate that privacy is of paramount importance to the American people. It is a freedom that we take for granted, but it is threatened by those who would use information in a brokered capacity from Internet sites and other devices to undermine privacy, and I think this hearing is right on point.

I think the legislation that has been developed is interesting, and a useful contribution to this debate, and I want to thank the commissioners for coming today and for their contribution.

[The prepared statement of Senator Dorgan follows:]

PREPARED STATEMENT OF HON. BYRON L. DORGAN, U.S. SENATOR FROM NORTH DAKOTA

Mr. Chairman, I am pleased that you have called this hearing on the subject of online privacy. In my judgment, the issue of online privacy is one of the most important and essential issues related to the Internet and e-commerce. It is very important that this Subcommittee follow this issue closely and seek appropriate solutions to ensure that consumers can have confidence that their privacy will be protected online.

While the Internet and online commerce provides enormous opportunity for communication, information collection, and commerce, it also provides an equal potential for serious invasion into people's rights to privacy. For this reason, the protection of privacy over this exciting new medium is of critical importance.

I greatly appreciate the work that the Federal Trade Commission has done on this important subject. However, the recent report on "Self Regulation and Privacy Online: A Report to Congress" highlights the fact that, at the present time, online privacy protections industry wide leaves a lot to be desired. I can appreciate the position of the majority of the Commissioners that legislation would be premature at this time. Nevertheless, I still believe that it is very important that Congress closely examine online privacy issues and debate over legislation is an important debate to have at this point. The findings of the Georgetown Internet Privacy Policy Survey that only 10% of Internet sites are implementing a full complement of online protections (such as notice/awareness, choice/consent, access/participation, and security/integrity) is very disturbing. It would be foolish to declare victory at this stage. In fact, we ought to remain very concerned and realize that there is a great deal of improvement needed in order for consumers to feel confident about privacy online.

Certainly, the industry has demonstrated that it is not deaf to the concerns of protecting privacy. Indeed, the industry has a strong self-interest in ensuring privacy protection and there is considerable evidence of industry-initiated efforts to adopt privacy protections. The industry has indeed come to the table to address privacy issues on their own to a large degree. But, if consumers loss confidence in their ability to protect their privacy online, they will likely leave the Internet and e-commerce

behind. The government ought to be just as concerned about a loss of consumer confidence in privacy protection as the industry. That is why much, much, more needs to be done.

I still have an open mind as to whether or not legislation is necessary at this point in time. But, I consider the debate a healthy one and I think at a minimum, this Committee ought to monitor the progress of the industry to adopt privacy protections. In the meantime, it is important that the FTC continue to work closely with industry to address online privacy issues. That relationship appears to be producing good results, but I remain concerned that that may not be sufficient in the long run.

Thank you Mr. Chairman. I look forward to hearing from today's witnesses.

Senator BURNS. Senator Rockefeller.

**STATEMENT OF HON. JOHN D. ROCKEFELLER IV,
U.S. SENATOR FROM WEST VIRGINIA**

Senator ROCKEFELLER. Thank you, Mr. Chairman. Just a brief word. I am still unclear as to how I feel about this, and I think reasonable people in fact in some ways ought to be unclear. I do not think enough people know enough about what the potential is for self-regulation, or what the lack of potential is for self-regulation.

I think the Georgetown study which the FTC used, used in fact to draw one set of conclusions, and one might argue that in fact it drew another set of conclusions, but that aside, it laid out five basic criteria that have to be met, and to me it is the meeting of the criteria more than the way in which they are met, whether it is done by Federal regulation or whether it is done by self-regulation.

Senator Wyden and I disagreed on the passenger bill of rights. I thought it could be done by self-regulation, he felt it should be done by legislative regulation, so these are in some ways, you know, similar, and philosophically they have a touch point, but I think the five points are, notice that information is being collected, choice of whether to disclose information, access to their own, that is the user's own information, security so that information is protection, and contact information for questions or complaints.

Now, whether or not in what we hear and talk about today the industry feels that they can do that, the record so far is not a very good one. On the other hand, the industry is yet a very young one, and laws last a long time. The industry changes and is capable of changing much more rapidly than are laws usually around here.

So I am reserving my right to hear some debate and decide what to do. I do, however, applaud your instinct for looking after the consumer, and I thank the chairman.

Senator BURNS. You can probably make up your mind by noon today. We do not want to push you too far. [Laughter.]

Let us continue on with the panel. From the Federal Trade Commission, the Hon. Sheila Anthony. We look forward to your opinion on this. Thank you for coming this morning.

**STATEMENT OF HON. SHEILA F. ANTHONY, COMMISSIONER,
FEDERAL TRADE COMMISSION**

Ms. ANTHONY. Thank you, Mr. Chairman, and members of the Subcommittee on Communications. I am delighted to be here this morning, and I appreciate your holding this hearing to address a topic of extreme importance to the American people.

As the commission's 1999 report to Congress states, only 10 percent of well-traveled Internet sites in a recent survey have privacy disclosures that speak to all four substantive information principles, notice, consent, access, and security. Even among the top 100 most frequently visited Internet sites, and I would think there are about 7,500 sites that are traveled, only some 20 percent have privacy disclosures addressing these four principles.

Some industry leaders have undertaken significant efforts to protect online privacy, and let me name a few. Microsoft, Dell Computer, Disney Online, IBM, AT&T, Eastman Kodak, Fox Broadcasting, the Boston Globe, the San Francisco Chronicle, the Wall Street Journal, CyberBills, Educational Communications, Inc., Worldtravelcenter.com.

These self-regulatory efforts constitute a reasonable response to the widespread market demand for the protection of consumer privacy, and likely play an important role in the growth of electronic commerce.

In addition, the seal programs show promise, but some companies have made a business out of collecting, buying, and selling individually identifiable information online. I was shocked to discover shortly after I joined the commission that at least one of the several information brokers operating in the marketplace had my name, my husband's name, our address, the value of our home, our social security numbers and the years they were issued, our mothers' maiden names, the address we lived before coming to Washington, our two daughters' names, their husbands' names, their social security numbers, and every address they ever had lived, including our 3-year-old grandchild's social security number and name.

I might add that there were several mistakes in this report. We in the Government, and especially those of us who have gone through a confirmation process, and you who have stood for election, know what it is to have your private lives laid bare, but most Americans do not, nor do they want to.

I am disappointed that sufficient progress by industry has not been made toward the protection of online privacy under a self-regulatory approach. Such a lack of progress is surprising, given the commission's clear articulation of fair information practice principles in our 1998 online privacy report.

Even prior to my arrival at the commission, the agency had encouraged industry to adopt voluntary fair information practices. Secretary of Commerce Brown plainly expressed the fair information principles of notice and consent as long ago as 1995. These ideas are not brand new.

The self-regulatory environment has not advanced the ball as far as I would have expected. Thus, consumer privacy remains an issue about which 87 percent of online Americans, including me, are extremely concerned. Privacy is one of our most cherished freedoms. Too often, however, the debate about privacy and the protection of personal information that is surreptitiously gathered takes on an ethereal quality and looks for proof of direct harm. Direct harm is not necessary to justify fair information practices, but it is evident, for example, in cases of cyber stalking and identity theft.

The American public deeply values its privacy, quite apart from notions of direct harm. The studies of which I am aware consistently show a high level of concern about online privacy. For example, a study just released in April by Harvard, MIT, AT&T labs, and the University of California at Irvine, found, as I mentioned earlier, that 87 percent of Internet users were concerned about personal privacy threats.

One year ago, these concerns were held by 81 percent of Internet users, so over the years, public concern has increased, not decreased.

In reporting on the status of self-regulation and online privacy protection, the commission has fulfilled its promises to collect information and report to the Congress. I respectfully and affectionately disagree with my colleagues, in that I believe the time is ripe for Congress to enact Federal legislation to protect online consumer privacy, at least to the extent of providing minimal Federal standards.

As a whole, industry progress has been far too slow. Notice, while an essential step, is not enough if the privacy practices themselves are toothless.

I do believe Congress is the appropriate place for the debate on this issue, and I note that several bipartisan bills are pending in both the House and the Senate, including the Online Privacy Protection Act that has been introduced by you, Chairman Burns, and cosponsored by Senator Wyden. These bills can serve as starting points to craft balanced privacy legislation.

I am concerned that without widespread implementation of fair information practices, and absent effective privacy protections, several results are inevitable. First, the dissatisfaction of the American people will grow both in pitch and intensity, as it has in the past.

Second, a patchwork of State laws to protect online privacy will emerge. A number of States, including California, Colorado, Connecticut, Delaware, Florida, Louisiana, Maine, Massachusetts, Minnesota, Montana, Nevada, New Hampshire, New York, Pennsylvania, South Carolina, Tennessee, Virginia, Washington, and Wisconsin have moved in that direction.

Consider the confusing environment that could result for consumers online marketers and the courts under such a legal patchwork. Consider also the extreme burden on online businesses to comply with this patchwork of privacy laws.

Such businesses would be required to determine the jurisdictional reach of each State possessing such privacy laws, and to develop compliance strategies to satisfy privacy requirements of each jurisdiction. Further, the entire process may need to be repeated as line businesses grow and expand their product lines and as other States enact their laws. A single minimum Federal standard of online privacy would decrease the cost and complexity of compliance while simultaneously establishing essential privacy protections for online American consumers. Further, I believe that Federal legislation and meaningful self-regulation should operate hand-in-hand.

Third, I am concerned that the absence of online privacy protections will continue to undermine consumer confidence and hinder the advancement of electronic commerce and trade, specifically of

trade with the European Union and its 320 million customers. Some types of personal information, such as health and financial information, may require heightened privacy protections, but without the widespread adoption of fair information practices not even an across-the-board minimum standard of protection exists.

Let me conclude by saying I remain troubled by the results of the Georgetown surveys, which show much less progress than I had hoped. I am pleased to say the commission will continue its involvement in the privacy arena, and our report sets out a number of initiatives for the coming year.

Thank you for the opportunity to share my views.
[The prepared statement of Ms. Anthony follows:]

PREPARED STATEMENT OF HON. SHEILA F. ANTHONY, FEDERAL TRADE COMMISSION

I support the Commission's 1999 Report to Congress on Self-Regulation and Privacy ("Report"). The Report commends the seal programs and the few responsible industry leaders that have undertaken significant efforts to protect online privacy by adopting fair information practices in their online dealings with consumers. I agree with the report's conclusions that industry leaders must continue to encourage widespread adoption of fair information practices; focus attention to the substance of web site information practices; and work together with government and consumer groups to educate consumers about privacy protection on the internet. I also support the Commission's agenda to address the public's strong concern about online privacy.

I am dismayed, however, with the results of the two studies cited in the Report. According to the studies, there is an enormous gap between the online collection of individually identifiable information and the protection of that information by the web site owners' implementation of fair information practices of notice, consent, access, and security. While 93 to 99 percent of the surveyed sites collect personal information from consumers, only 10 to 20 percent of these sites have privacy disclosures implementing the four basic substantive fair information practices.¹ It is not hard to see why surveys show that the vast majority of Americans are concerned about threats to their privacy online.²

I disagree with the majority's opinion that "legislation to address online privacy is not appropriate at this time."³ As a whole, industry progress has been far too slow since the Commission first began encouraging the adoption of voluntary fair information practices in 1996.⁴ Notice, while an essential first step, is not enough if the privacy practices themselves are toothless. I believe that the time is ripe for federal legislation to establish at least baseline minimum standards upon which meaningful self-regulation can flourish. I note that bipartisan bills are pending in both the House and the Senate and could provide a good starting point for crafting balanced protective legislation. I am concerned that the absence of effective privacy protections will undermine consumer confidence and hinder the advancement of electronic commerce and trade.

Senator BURNS. Thank you, commissioner, and Senator Kerry, do you have any questions of this panel? You will submit them, okay. Thank you very much. I know you have got other things to do. We are just trying to accommodate you.

Hon. Orson Swindle. Commissioner, we are looking forward to your comments this morning. Thank you for coming.

**STATEMENT OF HON. ORSON SWINDLE, COMMISSIONER,
FEDERAL TRADE COMMISSION**

Mr. SWINDLE. Thank you very much, Mr. Chairman, members of the committee. Let me begin by painting a big picture. Last month,

¹See Report at 8-9.

²See Report at 2-3.

³See Report at 15.

⁴"Staff Report, Public Workshop on Consumer Privacy on the Global Information Infrastructure," (December 1996).

the University of Texas, backed by Cisco Systems, introduced a study of the current status of electronic commerce as one of the very first efforts to measure the Internet economy. According to the study, the Internet economy generated an estimated \$301 billion in revenue in 1998 and was responsible for over 1.2 million jobs. These estimates are based on worldwide sales of Internet-related products and services by U.S.-based companies.

To put the figures in perspective, the Internet economy is already bigger than the energy industry, the telecommunications industry, and almost as big as the automobile industry. According to Secretary of Commerce Daley, retail consumer purchases over the Internet were \$3 billion in 1997, \$9 billion in 1998, and are estimated to approach \$30 billion this year.

We are witnessing an incredible economic engine just revving up. Consumers are not timidly engaging in this new form of commerce. As Chairman Pitofsky testified recently, it is remarkable the extent to which people are becoming committed to doing commerce on the Internet. Consumers seem to like it.

The Commission's 1999 report on privacy recently submitted to Congress ultimately reached the correct and obvious conclusion. No legislative action is necessary at this time. Significant self-regulatory progress has been made, but continued vigilance is needed if we are to obtain higher and higher levels of confidence in protecting personal privacy.

The path to those higher standards is not through more laws and regulations. Rather, industry, advocates for privacy and consumers and the Commission should be able to make further progress by continuing to work together towards what we all agree to be mutually beneficial goals.

Industry, however, must lead the way, and I am confident that it will, and will do so far more effectively than will more laws and bureaucratic decisionmaking.

There is an incredibly exciting new world of economic and educational power before us. The rapid convergence of technology, information, and entrepreneurship is ushering in one of the greatest expansions of freedom, choice and independence mankind has probably ever seen, and democracy will be better for it. However, without personal responsibility, democracy cannot flourish. Consumers definitely have a role to play.

For certain, there are hazards associated with this new environment. How we balance protecting consumers and at the same time make it possible for this vast potential to develop is critical. As reflected in our 1999 report, there is broad agreement on the core principles of fair information practices, notice, choice, access and security. S. 809 addresses each of these principles.

However, for those who wish to regulate online privacy, I ask how will we do it? The devil is always in the details. We are coming to realize that technology and cost, not to mention the exponential growth of the online world, are serious impediments.

Recent data suggest that there are now approximately 3.6 million commercial Web sites, and they are increasing at over 275,000 a month. We have a lot to learn about the Internet economy and how to deal with it, as our ongoing rulemaking to implement the Children's Online Privacy Protection Act of 1998 is revealing.

The old adage of looking before we leap is still wise advice. Imposing additional laws and regulations on that which we do not yet fully understand could produce incredibly negative unintended consequences. Imagine this scenario, if you will. First of all, massive numbers of unintended or innocent violations of the new law will likely occur. Commercial Web sites are increasing at almost 10 percent a month. The overwhelming majority of these violations would be by entrepreneurs seeking to market a product on the Internet without understanding the new requirements, or not possessing the technology or the resources to comply.

The regulators, armed with the new law, would, of course, have to enforce it. Imagine the scope of this task and the likely effects on entrepreneurs. While this might be a nightmare for regulators, it pales in significance to the possibility of regulation impeding the growth of this economic engine.

Do I suggest throwing in the virtual towel? Certainly not. I suggest a different approach driven by practicality. More law and regulation will not solve this problem. It is in the interests of businesses, large and small, to provide customers with safe transactions and secure privacy and business practices to win the confidence of those customers.

Because we are making progress, and because none of us fully understands where electronic commerce, entertainment, knowledge, information and education are heading, I strongly urge a more cautious approach. The rule of "do no harm" seems most applicable here. Let us not add more laws and regulations at this time. Rather, let us continue to work together and allow this new economic engine and privacy policies to evolve.

For the most part, businesses have the creativity and motivation to lead the way. Companies like AOL, IBM, and Microsoft, who have led the way, also help countless other companies by their example.

Organizations and seal programs such as the Direct Marketing Association, BBBOnline, TRUSTe and others also are leading the way, and progress is increasing day by day. Continued focus on the problem by the Congress, the commission, advocates for consumers and privacy, and leaders in industry should bring about the progress we desire and the sound balance that is imperative.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Swindle follows:]

PREPARED STATEMENT OF ORSON SWINDLE, COMMISSIONER,
FEDERAL TRADE COMMISSION

I have voted to submit "Self-Regulation and Privacy Online: A Report" (the "Report") to Congress, although I have done so with great reluctance. I have voted to submit the Report because we promised the Congress last summer that we would make a recommendation regarding the need for legislation addressing online privacy. *I also have voted to submit the Report because it ultimately reaches the correct and obvious conclusion: **no legislative action is necessary at this time.***

I must add, however, that I do not believe the Report accurately reflects reality. First, the dated and unfavorable results of the 1998 FTC Study are prominently described in the first seven pages of the Report, while the current and favorable results of the 1999 Georgetown survey are relegated to a brief discussion in the middle of the Report. Thus, the Report does not present a clear and complete picture of the substantial progress industry has made in the past year.

Second, the Report overemphasizes the failure of industry to sufficiently implement all elements of comprehensive "fair information practices." The Commission

first articulated the elements of these four practices in detail just one year ago. Given the recent vintage of these elements, I believe industry has made substantial progress on them as well.

Third, the Report only sparingly mentions the leadership on privacy issues that IBM, Microsoft, Disney, AOL, The Direct Marketing Association, privacy seal organizations, and many others in the private sector have continuously demonstrated. Faint praises tend to be damning. Industry's leadership in achieving progress should be lauded not buried.

Because the Report provides an inaccurate assessment of the current state of on-line privacy and of the substantial progress attributable to industry self-regulation, it is perhaps not too surprising that the no legislative action recommendation appears at the very end of the Report, almost as if the recommendation is some trivial afterthought. The Report instead should have emphasized "front and center" that cooperative and creative efforts by a public private partnership have achieved and will achieve progress far more quickly than more laws and regulations, which, while they may have a "feel good" quality to them, likely will have adverse unintended consequences.

In summary, I think significant progress has been made, but continued vigilance is needed because we are not where we want to be. The way to get where we want to be is not through more laws and regulation. Rather, industry, privacy and consumer advocates, and the Commission should be able to make further progress by continuing to work hard and work together. In the event that our joint efforts do not produce results, I would caution industry that there are many eager and willing to regulate. If industry wants to have the freedom to adopt privacy policies in response to market incentives and not government regulation, I encourage industry to continue to lead the way.

Senator BURNS. Thank you, commissioner. Now, Commissioner Mozelle Thompson, we thank you for coming this morning, and we are looking forward to your comments.

**STATEMENT OF HON. MOZELLE W. THOMPSON,
COMMISSIONER, FEDERAL TRADE COMMISSION**

Mr. THOMPSON. Thank you, Mr. Chairman. I am pleased to appear today before the Communications Subcommittee with my fellow commissioners to discuss the FTC's latest report on online privacy. As you are aware, we have spent a lot of time and energy working on this issue, and we welcome the opportunity for each of us to share our individual views and insights.

Following our 1998 report, in which the commission expressed disappointment about industry progress on self-regulation, I specifically voiced my concerns about coverage, which is the breadth of total Web sites actually posting privacy policies, and the development and implementation of enforcement mechanisms.

Now, 1 year later, and 3 years after the FTC first started working with industry on Internet issues, I find the record of progress is mixed. If we are going to be a leader in the global system of electronic commerce and e-commerce is going to continue to lead the new economy, we must reach a collective understanding on the principles that will provide consumers with the confidence they need to accept e-commerce as a way of life.

Those principles include the protection of consumer privacy. In that vein, I note that S. 809 incorporates each of the fair information principles the commission itself outlined in its testimony before the House Commerce Committee in July 1998.

During the past year, industry leaders have expended substantial effort to build self-regulatory programs. However, as the Georgetown and OPA studies clearly show, while many leading on-line companies understand the importance of the business case for protecting consumer privacy, implementation of fair information

practices is not widespread among commercial Web sites. In fact, a mere 10 percent of companies in the survey have done so.

Although the OPA does not audit its members for compliance with its privacy guidelines, the results of its own study shows that only 22 percent of the top 100 Web sites, most of which are OPA members, have implemented all four elements of fair information practices.

These findings suggest that even these industry leaders are only slowly rising to the challenge they have set. Accordingly, the most important challenges to be addressed include first, reaching those businesses which have not take steps to protect consumer privacy, especially small and medium-sized businesses, which we hope will provide the base for real growth in electronic commerce and, second, encouraging widespread adoption of all of the fair information practices, including educating consumers about the value of their own self-regulatory efforts.

The activities of the commission, and the ones that we have planned for the coming months, are designed to help us pinpoint specific problem areas for action. The information we uncover in these workshops and task forces will go beyond the simple quantitative analysis we have done on a number of sites with privacy policies to tell us exactly which aspects of fair information practices are not being complied with and why.

And so, despite my reservations and concerns about the pace of industry progress on privacy, I believe it is appropriate for us to defer making a legislative recommendation, because the commission's upcoming work will assist us in suggesting a more tailored legislative response if industry fails to make further substantial progress.

However, I will note that congressional review of privacy issues is also helpful, and I feel strongly that there is a value to continued hearings and debate about legislative proposals. I continue to be hopeful, as well, that industry can solve this problem. Recent initiatives by IBM, Microsoft, Disney, and the Direct Marketing Association are steps in the right direction.

I would also ask industry to redouble its efforts to develop effective technological tools that consumers can use to safeguard their own privacy online, because even well-crafted legislation will not achieve 100-percent compliance with fair information practices.

Ideally, easy to use technology will empower consumers by allowing them to predetermine the circumstances under which they will share their personal information. We heard about some of these technologies last week during our workshop on implementing the Children's Online Privacy Protection Act, and I am pleased to note that one of our proposed workshops for the coming months focuses specifically on these new tools.

In sum, achieving a robust level of privacy protection will require cooperation between industry, Government, and consumers. While we have chosen to let industry lead in solving this public policy problem, public confidence in electronic commerce will erode if they fail to live up to the challenge.

Ultimately, Government officials like us are directly accountable to the public, and we must also continue to play a role in shaping the solutions to the privacy problem. In any case, the FTC will con-

continue to pursue its enforcement role against those who deceive consumers by misusing their personal information.

I believe that self-regulation will succeed only if industry acts on the specific shortcomings documented by the recent studies. Moreover, Congress and the Administration must remain vigilant, and should not foreclose the possibility of legislative and regulatory action if there is not swift and significant additional progress.

Thank you.

Senator BURNS. Thank you very much, commissioner. I just have a couple of questions, then we will get into a little discussion and interaction here among our colleagues.

None of the studies referenced in your report provided recent data much beyond the top 100 Web sites. Do you have any data or experience about what is happening at lower levels, or do we go on beyond the 100 that were mentioned in your report, and that is for any commissioner who wants to address it.

Mr. PITOFSKY. Mr. Chairman, actually the Georgetown study has two sets of conclusions. One deals only with the top 100, but the other is a sample of a much broader range of Web sites, so that the Georgetown study does examine a very wide range of Web sites. It is the broader study that concluded that at least right now 66 percent of those Web sites have some kind of privacy policy on their screen.

Mr. SWINDLE. I think one of the critical points in looking at this kind of an evaluation is, as I mentioned, there are several million commercial Web sites, and by no stretch of the imagination have we looked at all of those, and it sort of makes the point I was trying to get to.

But the sites that we looked at in the survey, or at least Professor Culnan looked at in her survey, looked at sites which encompassed an extremely high percentage of all the people who looked at the Internet, so it is not so much the universe of sites as it is where you are touching the most people. I think that was the purpose, as I understood it, of the approach in the survey, to look and see what is happening on sites where the vast, vast majority of people were looking, and I think that figure exceeded well over 90 percent.

Senator BURNS. Any other comments?

Mr. THOMPSON. Just from the tenor of your question, though, I think one of the issues that I would be concerned about, and one that I think we want to get at through further study, is there a core that we are not getting to, those who are maybe well-trafficked but are still not doing what they should be doing in terms of privacy policies, and what are the impediments there?

I think that at least from my standpoint would lead me to recommend, if necessary, the kind of tailored legislation that gets at the problem, but that is one of the issues that I am concerned about, especially if we are going to see real growth, and we are sensing that now in midsized companies, not just the industry leaders, but in a broader base of e-commerce.

Senator BURNS. Can you describe how S. 809 is philosophically different from the Children's Online Privacy Protection Act that we passed last year that causes you concerns? Philosophically, how are we different in that bill that we passed a year ago?

Mr. PITOFKY. I think S. 809 looks in the same direction as the children's statute. It has a balance to it that I really admire, and it seems to be organized in such a way as to create incentives for industry to respond on their own.

I also like the safe harbor provision that is in the bill.

My own view is that the idea of commercial Web sites invading a family's privacy by taking advantage of kids, of 8, 9, 10-year-olds, is so outside the acceptable commercial behavior that to me, of course, you should have legislation.

That is intolerable and, indeed, 2 of the 3 major cases that we brought challenging companies for their behavior invading privacy involved invading privacy of kids. It was Senator Bryan and you among others who really led the way in getting Congress to act in that area.

With adults as well, I think invasions of privacy are unacceptable. But, we are not talking as we were in the children's statute about putting parents in control of their children's behavior when they are engaged in commercial behavior on the Internet. We are certainly not talking about companies essentially saying to the parents, "Why don't you wait outside while we deal with your children?" While you "wait outside" we will enquire for example, what their grandparents give them with respect to stocks last Christmas, what is the income of the family, that sort of question.

That invasion of a family's privacy seems to me utterly unacceptable, and that is the reason why we supported legislation there. I feel the same about privacy connected with financial records, medical records. Here, it is a tougher question.

Senator BURNS. Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman.

Senator BURNS. I guess I went out of order. It should be Senator Bryan. I am sorry.

Senator BRYAN. I appreciate that, but I would defer to Senator WYDEN. He is a cosponsor of the legislation. Go right ahead.

Senator WYDEN. I thank my friend for his graciousness.

Mr. Chairman, so many nice things have been said about S. 809 in the last half-an-hour I am tempted to say we ought to quit while we are ahead and just go forward, but I would like to ask about a couple of issues, and let me direct this one to you, Mr. Pitofsky.

The commission said last July, and I quote here, unless industry can demonstrate that it has developed and implemented broadbased and effective self-regulatory programs by the end of this year, additional Government authority in this area would be appropriate and necessary, and I would like to begin by asking you if you think that the Georgetown study met the test that the commission laid out a year ago.

Mr. PITOFKY. I do not believe that industry self-regulation is nearly where it has to be in order to persuade all of us that legislation is not appropriate.

I do believe that the progress they made in 1 year is surprising to me, and impressive.

Senator WYDEN. If a company publishes a privacy policy which provides consumers with no choice, and that company collects and resells personal information about their customers, in your view does that provide adequate privacy protection for the consumer?

Mr. PITOFSKY. I do not think so. I know there is a bill that says, put up a privacy policy, it does not matter what it says, just put something up there and that will satisfy the law. I think consumers are entitled to better than that if we are going to go the legislative route.

Senator WYDEN. In your opinion today, does the FTC have the authority to take any action in those kinds of cases?

Mr. PITOFSKY. Where they put up no policy at all? I do not think we do. We put out an advisory opinion that perhaps we could act where the victims were children, but if the victim is an adult, we could take that case to the courts and maybe we could win it, but it would be beyond the precedent base of our unfairness jurisdiction as it now exists.

Mr. SWINDLE. Senator Wyden, may I comment on that? You characterize this as a consumer having no choice. The consumer always has a choice. It is simply to click. That is what is so marvelous about the Internet. It is perhaps the ultimate of free expression and choice. The consumer does not have to be there if they do not like what they see, or they do not like the products they get, they do not like the prices, they do not like the questions being asked.

I know I personally, on one of the major newspapers, I log on because I read most newspapers by the Internet, the site started to ask me a bunch of questions. After I got by my name I said, I am not going to answer these questions, so away they went, and now I look at it in print form, although the ink makes me sneeze, so I am still not too happy with them, but I just simply will not deal with the website. Apparently, I have forgotten which Senator mentioned that a survey recently of major CEOs, 60 percent of them said they do not give personal information either. That is choice.

As to Senator Burns' comment about the philosophical differences between the online children's privacy and what we are talking about here, I think it is a matter of we are dealing with children in one case and adults in another.

As I commented in my earlier comments, democracy depends on individual responsibility, and so we are never without choice, and we will never reach perfection in this. No law ever does reach perfection, but I would contend, looking at the numbers, that we are going to have even a harder time with this one.

We could always look to the example of the Soviet Union. They virtually, or at least claimed to have perfection. They had no freedom, but they had perfection. They did not have much crime.

So I think these kinds of things have to be taken into consideration.

Senator WYDEN. I think what the debate is about, commissioner, is whether people have an informed choice, and to me capitalism and making free markets work only can go forward when people can get information so they can make an informed choice. There is no debate at all about the fact that you can click the button.

The question is, can you have enough information so that when you are making those choices with the clicks, they can be informed ones, and that is why I come to this as one of the coauthors of the Internet tax freedom bill, and Y2K liability, and encryption, and a whole host of other things, making it very clear I am not some

wild-eyed fanatic for regulating the Internet and running some kind of one-size-fits-all Federal operation from Washington, D.C.

I am just very troubled by the fact that I do not think in a lot of instances people are getting the information to make choices, and what Bob Pitofsky essentially said is, he is concerned about the problem. We can debate about what to do about it, he does not think the commission has the authority to do what I think is important for the bad actors that I know you are concerned about and I am concerned about, and that is what we are wrestling with, and that is what we are trying to strike the balance on.

Now, just a couple of other questions, and any commissioner really can get into this. My understanding is that, as of today, it is still a small number of Web sites that actually belong to one of these seal programs, one of the programs to try to have the self-regulation that we have commended the larger companies for.

Now, again, as with all of this, you have to put it in context. If you go on aggregate number of hits, it seems to me we are just as Bob Pitofsky said, we are making some progress, but if we have got a lot of people out there running Web sites without any effort to belong to these seal programs, that troubles me as well.

Is it correct that it is a pretty small number of Web sites belonging to seal programs?

Mr. THOMPSON. I think the answer is yes. I think that is one of the challenges for the industry, is to figure out how they can broaden that coverage, but it also points out, without trying to cast a shadow on S. 809, but some of the areas that I would like more information about in order to better, if I were making legislative recommendations, to better tailor it. One is, what is the size of that core, and is there something in legislation that would be more directed at getting at that problem? That is number 1.

Second of all, with regard to the safe harbor, I really think that industry members, who are doing a good job, should be getting the benefit of that safe harbor, but it is hard to tell from at least where I stand at this point how broad that safe harbor should be, who it should cover, and under what circumstances. That is some of the information I would like to find out as our further study commences.

Senator WYDEN. That is a fair comment, and I can tell you that Senator Burns, as we worked on the legislation and as he and I talked to folks in the industry, it is our desire to ensure that there is a wide birth for self-regulation. I mean, we want to make sure that that safe harbor is done right, and Bob Pitofsky and I have talked about it. We would very much appreciate the counsel and the input of the commission and the good folks that you have over there to do it right, because we want to give a wide birth for that, and to let the broadest possible set of self-regulatory efforts go forward.

A last question I have, and again I am taking time from Senator Bryan—

Senator BURNS. I am going to cut you off here.

Senator WYDEN. Can I just ask one other real quick one? Given the fact that now the FTC has said they do not have much authority—we have got a small number of Web sites belonging to a seal program.

What we are saying is that there really is almost a pattern of nonenforcement of what is out there today, and I guess the last question for any of you, given the fact that we are trying to deal with the bad actors, it seems to me you do need some enforcement authority to deal with those kinds of people. Is there anything else that might possibly be an enforcement tool against people that all four of you would say are sleazy and are not in line with the principles that we would like?

Mr. THOMPSON. Money. That would help.

Mr. PITOFSKY. Let me start out, first, I hope I have not left the impression that we are helpless to address the problem created by the irresponsible few on the Internet. That is not quite the case. We have brought 91 cases in less than a year challenging fraud on the Internet, and several involving privacy invasions on the Internet, so if they deceive people, they say give us the information and you can count on us, we will not abuse the information that you give us, we bring those cases.

Now, second, as more and more companies put a privacy policy up on the Internet, to the extent that they do not abide by their own policy, that would be deceptive and we would challenge that.

Now, many of them, more than half have privacy policies now. My hope is, and maybe I am being unduly optimistic about this, is they will have as good a year this year as they did last, and we will be up to the point where something like 90 percent of the companies will have a privacy policy, and if they do not observe their own commitments, then we are not helpless to act. We would challenge that kind of behavior.

Mr. SWINDLE. Senator Wyden, on one point, I think this whole process is evolving. As Senator Rockefeller I think said earlier, we are just in the embryo stage of this thing, realizing that Netscape came along here, the browser, what, in 1993 or 1994 I believe, and we have gone from having 50 Web sites in 1993, I think I heard yesterday at a conference, to having 5 million plus now, or 6 million.

I think we make a mistake by assuming that those who do not have privacy policies are bad. That takes us to places I do not think we need to go.

Second, when we judge the progress by the number of people who are on the seal programs, or coming under the seal programs, BBBOnline, or TRUSTe and so forth—there are many extraordinarily good companies, I suspect. I do not have the numbers, and I have written myself a note to find out—that have privacy policies that are probably very good, but who are not members of one of the seal programs. So, I just think we have got to look at the big picture here and not just pick out one thing and say, BBBOnline has only got X number of members.

Thank you, sir.

Ms. ANTHONY. I would just like to make this point. Federal legislation setting out minimum standards and industry self-regulation are not mutually exclusive. Our own FTC act, which requires that advertising be truthful and nondeceptive, which the Congress in its great wisdom passed some many years ago, still has engendered a very robust self-regulatory program by the advertisers of America,

and they work with us on a very constant basis in seeing that advertising in the United States is on sound footing.

Passing minimum standards here to protect consumer privacy does not spell the death knell for self-regulatory efforts. In fact, I should hope they would be enhanced from that starting point.

Senator WYDEN. I took a lot of time. Thank you, Mr. Chairman.

Senator BURNS. I would have to say that this business probably is not any different than any other business, and I was struck by the comment of Mr. Swindle who says, how do you find a balance that you do not kill the enthusiasm of this economic engine and still give the consumer the protection that he deserves, and that is a very fine line.

Senator Bryan.

Senator BRYAN. Thank you very much, Mr. Chairman, and to each of our distinguished witnesses, thank you very much for a very thoughtful dialogue today. I think this is very helpful.

I continue to be dazzled and amazed with the extraordinary explosion of information-gathering capability. In this article that I mentioned briefly in my opening comments, it goes on to point out that one Web portal acquires 400 billion bytes of information each day.

Now, I think for most Americans the definition of a byte is not something that is probably the discussion at dinner time conversation, but we are told here it is the equivalent of 800,000 books that would be placed in a library each day. I recognize it as a very difficult concept to fully get our arms around and to do the right thing, but let me say, Chairman Pitofsky, with whom I have had a wonderful working relationship, and I do very much appreciate, it does strike me as a kind of a follow up to Senator Wyden's question, that we do have a catch-22.

You are saying, and I think that is correct, that those Web sites that publish privacy standards, that if they violate that, that you have the ability under, I think it is section 5, to enforce that. Yet for the rogues out there in the world, if they have no privacy standard, it would seem to me that you have no capability at least to operate under the premise of a deceptive trade practice.

Is that not a kind of a catch-22? The very people that we probably want to bring on board because there are a number of responsible Web operators who are moving in the direction that we all want. Let me give you an opportunity to respond to that, the catch-22 syndrome.

Mr. PITOFSKY. I think the point you make is very well-taken. It is a problem. I think I would like to join my colleague, Commissioner Thompson. What we want to find out a little bit better is, who are those people out there? It is possible that the people who are gathering hundreds of thousands of pieces of information, they are the ones that have privacy policies.

The 34 percent that do not is somebody operating in their backyard on a narrow range selling some food product or some record or some book. They do not have the kind of information that anybody would buy anyway.

But we do not know the answer to that. I am not asserting that. I am saying, I want to find out more about it.

Let me just say, I want to share the view of my colleague, Commissioner Anthony, that this is not either-or. Self regulation and legislation have to mesh. What I am saying is that we would know more, be in a better position to decide what minimum standards ought to be, after we study this area a little more and get some more information.

Senator BRYAN. Mr. Swindle, if I might be able to respond to a comment you made and give you an opportunity to respond to my comment, you have unfurled the banner of choice. That is the essence of the greatness in America, it seems to me. We have a lot of choices, and the entrepreneurial genius of the free market systems provide us a range of choices that are beyond what any of us could have imagined a decade ago, much less a half century ago.

But you said the choice, you can dial up on the Web, and if you do not want it, you do not have to, but that does ignore one aspect that is particularly troublesome to me, and that is this concept of cookies, these Web sites that put these tags on. I think most people have no idea that by simply browsing, all of a sudden information can be captured with respect to them. How do you respond to that issue, because that is not choice.

Mr. SWINDLE. Senator, I totally agree with you. I think what you are speaking of, the consumer's lack of knowledge or now the acquiring of knowledge is reflected somewhat in the statistics that Commissioner Anthony used a little while ago, when she said a survey was taken last year and said that 81 percent of the people were concerned about the privacy on the Internet, and a more recent study said 88 percent are concerned.

I would contend that is because they now have more knowledge of what is possible through, as you describe, the cookie.

Again, as I tried to point out, we are in an industry that is evolving in every sense of the word. Awareness on the part of the public, consumer education, Government regulatory agencies trying to understand the phenomenon, businesses trying to understand the phenomenon.

I have been aware of this "Cookies" for some time, but perhaps I am a little bit better informed by circumstance. Certainly not by intellect, I might add, but certainly by circumstance, and I am highly offended when one of these sites starts asking me a question. I just leave them. I will not do it.

But when you do not know that it is going on you are being victimized, and I think if we get more consumer education out there, and people become more aware, we will see changes, and industry is going to recognize they have got to satisfy their customers.

Senator BRYAN. Do we have any idea how much information is collected through this cookies device, and what these Web sites are doing with it? Are they blending offline information, address, social security number, that sort of thing? I will just toss that out to any one of you who might care to respond. Do we have any information?

I find this particularly troublesome because in this sense, even the fairly sophisticated user of the Internet is captured. In other words, it is a gotcha. You dial up, and that information is captured. It is not a volitional choice as to whether or not you want to do

business, or to request information from the Web site. Is there any information out there that we have?

Mr. PITOFSKY. You asked two questions. One is, do we have any sense of how much information is collected surreptitiously, not just about what you buy, but what you think of buying, what you are browsing. My answer is we do not. At least, I am not aware of it. I think frankly this exchange suggests to me that in our report we ought to address that issue. Either we know that answer, or we should say we do not.

As to your other question, I think we do know that companies are blending online and offline information in something called profiling, identity profiling, and that is very troublesome, too. Commissioner Anthony read that long, long range of information that is being gathered about people. I think quite frequently that includes online and offline sources of information, and it is a subject that ought to trouble all of us.

Senator BRYAN. And finally, let me just ask a question that is just a bit off the beat, but I think raises some policy considerations.

Sometime back we had a hearing before this committee on broadband technology, and I recall the AOL person who testified raised the issue that was described essentially access is gained through the telephone system or cable, and that through the telephone system we have a common carrier concept. Everybody kind of has access to it, and a level playing field, whereas with respect to cable that is not the case. The AOL representative I thought made a fairly persuasive point that that is something we need to take a look at.

Now I read in the newspaper fairly recently that two of the titans in the industry, Microsoft and AOL are going toe to toe with respect to this instant messaging concept, and Microsoft comes out with the software that will allow their users in effect to communicate with the AOL instant messaging subscribers, and now AOL counterattacks by blocking access, and now Microsoft is indicating that they are going to come back with some kind of a counter to that counter.

Are there not some public policy implications? I mean, if we were back in 1876 after Alexander Graham Bell asked Mr. Watson to come here, that the idea that somehow we would allow in the 20th Century. You cannot gain access to another telephone system I think would come as a shock to us.

What are the policy implications for us there? I am talking about consumers, recognizing there are some legitimate proprietary interests. I am not sure I have got the answer, but you all give a lot of thought to these kinds of things. If I could invite your response, and I thank you, Mr. Chairman

Mr. PITOFSKY. Two reactions. No. 1 is, you are absolutely right to put this issue in the much broader context of where we are going structurally in communications technology.

No. 2, I am going to duck and say, we may take a look at this question, and if we do I do not think I should be speaking out on the issue at this time.

Senator BRYAN. Well, we may read something into that. Thank you. [Laughter.]

I think that is a subliminal message. I would invite anybody else to respond. Silence reigns in the valley.

Senator BURNS. Being raised and living west of the 100th meridian, and dealing with the era that you were talking about, about this, I am afraid we would have another OK Corral to settle this.

Senator BRYAN. It could be another Little Big Horn, however. [Laughter.]

Senator BURNS. Senator Rockefeller.

Senator ROCKEFELLER. It is very interesting to me, just from the point of view of the nature of Americans, when you come to an issue like this. Justice Brandeis was terrified of the invasion of privacy when photographs came out, and now we are going through exactly the same thing, with the obvious difference that the reach of the Internet is far greater, far more pervasive, and far more damaging to privacy than obviously a photograph. Although photographs have done some fairly amazing things in American life.

I guess the question I would ask is, if less than 10 percent of Web sites are doing what is felt to be adequate, then one would come to the automatic judgment, well then, we have to do something about it.

Then on the other hand 82 percent of the American people are worried that their privacy is going to be invaded, and a lot of them say they would rather not even get on the Internet than take that chance. That would seem to go against the interests of the industry because that is like depriving themselves of customers if they do not behave as they should.

Frequently, industry wants to respond to its consumers, needs to respond to its consumers, and particularly in an industry like this one, where 9 out of 10 startup companies go out of business, which is higher than the usual. It is incredibly competitive, incredibly important to satisfy your users.

So that leads me to this. It would seem to me there is an incentive, which is called the market, more business for industry to do better, as, indeed, Microsoft and a few other companies are doing better, as the Georgetown studies and hearings like this in an incredibly young industry—remember, we did not have any Internet in the Senate until 2 or 3 years ago, so this is a very, very young industry. It would seem to be in the interest of industry to protect privacy to the extent that it can.

Now, I do not know what that really means, but I would be interested in your reaction, Mr. Chairman, and those of the other commissioners, of how at this very young stage you come to judge what the potential for this industry's behavior in response to this problem might be.

Mr. PITOFSKY. That is quite a challenge. My own sense, and I speak only for myself, is I think this industry does get it. Or at least, let me put it this way, I think the responsible leaders of this industry get it, and they know that it is in their interest to ensure to consumers that their privacy will be protected and to crack down if they can on those other companies who do not get it. I think they have worked hard in this area over the last year or so.

Are they going to accomplish all that virtually all of us in this room agree is necessary? I do not know, but I do think we ought to let this issue work its way out a little bit longer. We ought to

let a little time go by. If nothing else, we will have a better idea of what legislation we really need.

What is reasonable access? What does that consist of? What are security arrangements? How should we set up the safe harbors? We know a lot now. I think we will know a lot more in 6 months, 8 months, 10 months. We will certainly know whether this remarkable progress is going to continue.

Senator ROCKEFELLER. That is very interesting to me. I would have said 1 or 2 years, or 3 years, and you are saying no, a much shorter time. You are not for the legislative approach. You are for the self-regulatory approach.

But on the other hand, you are saying, if in a period of 6 to 8 to 10 months we do not see the protection of privacy that we feel that we need to meet the criteria, for example, that the Georgetown report talks about, then the FTC might change its view and take a tougher view.

Now, that is a very interesting time line. I mean, around here it usually takes 3 or 4 years to pass anything, and in fact, the chairman of this full committee is totally against the bill that the subcommittee chairman is for, and given the power of chairmen, the bill may never come up.

So it is philosophically within the American political context interesting to me that, do we go now for what we judge to be the right criteria and lay it down, understanding that what you put up on your Web site as labeling of your protection of your customers does not necessarily mean you have to follow through underneath.

I mean, Meg Widman to me is sort of the perfect example. Meg Widman is caught right in between with eBay, because she has to have information about her customers in order for her customers to trust each other enough in order to do business with each other through the medium of auctioning, therefore she has to have information. Yet, if she gets caught getting too much information, which is—not caught, but if she gets too much information and it goes beyond what competing potential buyers need, then she could be in some kind of trouble, so it is interesting to me that you say 6 or 8 or 10 months might tell us what we need to know.

My question from that obviously has to be, does that mean that 9½ percent of Web sites which now do provide that kind of privacy will—that that is going to increase enormously in 6 or 8 or 10 months, or are there discussions not only in the top 100 Web sites but in the whole industry? Are they ongoing to the extent that one could reasonably say, well, there are going to be substantial changes in the industry? The FTC would accept that position for the moment if they believe that there will be changes?

Mr. PITOFISKY. Let me respond, and I know my colleagues want to speak to your excellent questions.

Our report commits us. We will be back here with a report in less than a year. Now, a couple of months have gone by already since we wrote our report, so we are going to be back here soon. I do not think this is an industry where you wait around 3 or 4 years. It moves too quickly, and therefore I think we have a responsibility to have a followup report in this area.

Am I convinced that industry's word is good, and they will really achieve all these things? I am very interested in their commitments

and in their hopes and in their ambitions, but no, that is not going to be the answer. The answer has to be production of a privacy policy that satisfies as many of these goals as this group thinks ought to be satisfied.

I think things are going to get better. I think they will continue to improve. The way I put it is, will they get to the goal line? I don't know. They have a long way to go.

Mr. THOMPSON. I think you raise some excellent questions, and raise some of the concerns that I have.

First of all, one of the challenges that we are seeing is whether industry, the leaders in the industry can reach out and capture those who are not participating.

Now, we have to understand the impediments why they are not, but let me tell you there are some things going on right now that we think are very helpful. For example, when IBM and Microsoft say that they are not going to advertise on Web sites that do not have a privacy policy, and this is our strategy for moving in that direction, that is the kind of business-to-business initiative that moves in the right direction. That is one.

Second, is when the Online Privacy Alliance and others like the DMA say, if you do not have a privacy policy that meets these principles by X date, then you will no longer be a member of our association, that is another business-to-business kind of initiative that we think moves in the right direction.

Also, when they begin to say we are going to have a business education program that is going to have these kinds of milestones, those are the kinds of initiatives that are going to be important. We have to begin to measure those milestones and examine them carefully to see how they fit into a legislative recommendation.

In addition, there are other things going on at the same time that are going to be very important to this discussion. The fact that technology is going to be improving, we know that. There are some companies that we have heard of that want to provide consumers with tools so that they can decide how they want to use information. That is going to be factored in.

At the same time we have seen the movement of getting better technology to deal with cookies, not just the fact that the best that we have now is that when someone puts a cookie on your machine they tell you there is a cookie. It does not tell you what that cookie does. It does not tell what information they are gathering, though we have seen people working on technology to give consumers better information about what the nature of those cookies are.

All of those things are coming to a head, and where I share the chairman's view is this. Do not forget, 3 years ago there was no Amazon.com, so 1 Internet-year people frequently say equals 3 years of normal business time, so that if we are talking about compressed time frames here, I think that industry understands that, and we understand that as well.

Senator ROCKEFELLER. Commissioner Anthony, I apologize, but you might have a different opinion. If so, I would like to hear it.

Ms. ANTHONY. I think the leaders of business really have stepped up to the plate in many instances, but as Senator Wyden said earlier today, it is not the leaders of the industry that I am so terribly concerned about because they are attempting to be responsible.

It is the vast number of others who are gathering personally identifiable information and selling it oftentimes to people with whom the visitor to the Web site has not contracted for any purpose, or really has no idea that the information is being passed on to others.

I think that is the most offensive thing to me. I cannot speak for all Americans, but certainly that is very bothersome, very troublesome.

Senator ROCKEFELLER. Thank you all. Thank you, Mr. Chairman.

Senator BURNS. Thank you. I want to thank the commission.

Mr. Swindle, you said a while ago there is always the click. You can always click it off whenever you think—

Mr. SWINDLE. It is time to click.

Senator BURNS. Well, I can remember, and so can the rest of the members of this committee, when we were talking about the V chip, and ratings and things on television, and some inappropriate material that we thought should have some way to be identified and to be filtered and this type thing. Well, I always said there is a V chip on your television right now. It is called an on and off button, and I lost that argument, by the way.

But nonetheless, I thank you for your opinion this morning. It is really valued, and you have spent an inordinate amount of time dealing with this situation, and I appreciate that very much.

Are there any other Members that have other questions of the commission this morning?

I want to again express my appreciation.

Senator ROCKEFELLER. Can I ask one? You should not have asked that.

Senator BURNS. We almost made it, Mr. Chairman. [Laughter.]

Senator ROCKEFELLER. This in fact interests me very much, because recently the FCC—not FTC, but FCC ruled that all cellular phones must have the ability to give emergency personnel an exact location of a phone's user.

Just think about that. That means that anybody under a circumstance could be identified precisely where they are by law, by Government regulation, and that could be seen to be dangerous, and with far-reaching consequences.

I remember a number of years ago an enormous tree, 150-year-old oak fell on my wife and car, and she broke a lot of ribs and had a lot of damage done to her on a crowded parkway. It took an hour-and-a-half for an emergency vehicle to get to her.

Now, I am not saying with a crowded parkway that it would have been faster, but to know exactly where she was would have been good, and yet that also raises questions, I would think, with some of you. I am interested in the philosophical tug of that, with my apologies to the chairman.

Mr. PITOFKY. Very quickly, that is a tough one. I do not think this issue we have been discussing is nearly as tough as the one you raise, because there is a tradeoff on the issue you raise between the good things that are accomplished and the invasion of privacy. I mean, who wants the world to know exactly where you are every minute? I do not see this set of issues in that way.

Here, people are taking personally identifiable information, accumulating it, marshaling it, and selling it without your permission.

I do not see the tradeoff there. That should be prevented. The question is, how you do it.

Senator BURNS. I would draw a parallel. I can remember buying a toaster one time and it asked me all these silly questions when I sent back the warranty. If I wanted to get a warranty on that toaster, they asked me all these questions, you know, and there was no way to click off on that. I did not fill them out, and I did not get the warranty on the toaster anyway. I was going to use it for other than toast. [Laughter.]

I had another idea, and that did not work, either. [Laughter.]

Thank you very much. We appreciate the commission coming down this morning, and I will invite the second panel to come forward and take the table. We really appreciate your coming down today, because we know you have a busy schedule of your own.

We will now hear from the industry, and we would like to call to the table Ms. Jill Lesser, Ms. Deirdre Mulligan, Marc Rotenberg, and Ms. Christine Varney. They are representatives of the industry, and we are looking forward to their testimony.

OK, as we get situated we are looking forward to the views of the industry, and I would like to introduce at this time Ms. Jill Lesser, who is vice president, domestic public policy, America Online. Thank you for coming this morning. We are looking forward to your comments.

**STATEMENT OF JILL LESSER, VICE PRESIDENT,
DOMESTIC PUBLIC POLICY, AMERICA ONLINE**

Ms. LESSER. Chairman Burns, members of the subcommittee, thank you for the opportunity to discuss online privacy with you today. As Chairman Burns said, I am Jill Lesser, and I am vice president for domestic public policy at America Online.

Privacy is, as we heard in the first panel and as we have been hearing in the media, an extremely important issue, because the online medium is quickly revolutionizing the way people learn, communicate, and engage in business. People are migrating online to meet their commerce and communications needs, and there is an ever-increasing array of services.

The online environment also offers unique benefits for customization and personalization, and consumers can communicate specific preferences online that will allow them to receive products and information targeted to them.

For example, AOL members can set up their own online preferences, and I stress that they do this voluntarily, putting in their zip code from their home town, and they can receive weather and receive news stories in their local home town paper.

But the power of the Internet, as you have heard earlier today and as we have repeatedly said, can only be realized if consumers feel confident that their privacy is protected online and that they trust the entities with whom they are doing business and communicating.

We, as a company, have taken many important steps to create an environment where our members can be certain that their personal information is protected, and we protect the choices they make regarding that information. Building on the lessons that we have learned, sometimes from difficult experiences, and the input

we have received from our members and policymakers, many of you included, we have created privacy policies that clearly explain our policies to our users, what we collect, what we do with it, who we share it with, and how they can exercise choices.

The privacy policy that we have lately adopted is based on eight core principles, some of which are, we do not read any online private communications, we do not use information about where our member goes online for anything, and we do not share any of that information with others. We give choices to AOL users, and we take extra steps to protect kids.

We also make sure, and I think this is very critical, that the privacy policy we have adopted is implemented throughout the company and is signed by each and every one of AOL's employees, and we keep our users informed about how they can protect their own privacy.

For example, we constantly encourage—indeed, every time a member signs on, that they should not give out their personal information unless they know with whom they are dealing, and should never give out their AOL password to anyone.

As I said, we take extra steps to protect kids. That includes the creation of a kids-only area, and we did, as I will discuss later, support Senator Bryan's efforts last year in the Children's Online Protection Act, because we do believe there was an area of particular concern.

Going further than just privacy, and also just with respect to AOL proper, we have developed one of the strongest examples I think of consumer protection and privacy online with our Certified Merchant program, where we basically require all of our merchants, and that is all the partners who sell to consumers within the AOL shopping area, to abide by our Certified Merchant program, and that includes adopting their own privacy policy or complying with America Online's privacy policy in addition to engaging in other forms of consumer protection disclosures like making sure people understand what return policies are, when products will be shipped, and the like.

As you will hear from Christine Varney, we have been a leader in the Online Privacy Alliance, which has undertaken to promote market-driven policies in the area of privacy, and we also believe strongly that technology holds the key to ensuring a safe and secure online environment.

As an online service provider, we believe it is critical to be able to provide the most sophisticated security technologies to our members in order that they can help protect their own privacy, and we will, as we have in the past, continue to advocate strong encryption uses here and abroad.

Let me comment on the focus of today's hearing, and that is S. 809, the Online Privacy Protection Act. We would urge the committee, as I think the FTC has done, to proceed with caution in considering legislation, but we do not believe that our comments indicate that Congress should be any less vigilant in tracking industry's progress in identifying areas where legislation may be appropriate.

As I noted earlier, we did support the Children's Online Privacy Protection Act because of the unique concerns relating to child safe-

ty in the online environment. However, even that legislation, which was carefully crafted and widely vetted, is raising challenging interpretation and implementation issues for the Federal Trade Commission and the industry, and we are going to continue to work through that process.

With respect to the specifics of S. 809, I would urge the committee to consider focusing not on a regulatory framework, but on an enforcement framework. In that way, I think that the FTC can be empowered to stop the bad guys, in quotes, and let the good guys continue to serve consumers with innovative services and products.

What our research shows is that consumers are most interested in an honest exchange. They see the benefit of the services they receive online, but they want to ensure that they know who will have access to the information and what will be done with it, and so I think that focusing on giving the FTC the powers they need, as Chairman Pitofsky noted, to basically go after those folks who are engaging in fraudulent business practices, while not telling the leaders in the industry exactly where and how, for example, they need to post privacy policies, will be very productive discussion, and we look forward to engaging in that dialogue with you, Mr. Chairman, and with Senator Wyden and others interested in this important issue.

I appreciate the opportunity to appear here, and I am happy to answer any questions.

[The prepared statement of Ms. Lesser follows:]

PREPARED STATEMENT OF JILL LESSER, VICE PRESIDENT, DOMESTIC PUBLIC POLICY,
AMERICA ONLINE

Chairman Burns, Senator Hollings and Members of the Subcommittee, I would like to thank you, on behalf of America Online, for the opportunity to discuss online privacy with you today. My name is Jill Lesser, and I am the Vice President for Domestic Policy at AOL.

Privacy is an extremely important issue because the online medium is quickly revolutionizing the way we learn, communicate, and do business. People are migrating to the Internet to meet their commerce and communication needs at an extraordinary rate because it is convenient and fast, and offers an ever-growing selection of information, goods and services. AOL subscribers can sign on to our service and do research, shop for clothes, and buy airline tickets all in a matter of minutes.

In addition, the online environment offers users unique benefits of customization and personalization. Consumers can communicate specific preferences online that will allow them to receive information targeted to their own interests. For instance, AOL members can set their online preferences to get the weather forecast for their own zip code, read news stories about their own hometown, or receive notices about special discounts on their favorite CDs. No other commercial or educational medium has ever afforded such tremendous potential for personalization.

But the power of the Internet can only be fully realized if consumers feel confident that their privacy is properly protected when they take advantage of these benefits. We know very well that if consumers do not feel secure online, they will not engage in online commerce or communication—and without this confidence, our business cannot grow. For AOL, therefore, protecting our members' privacy is essential to earning their trust, and this trust is, in turn, essential to building the online medium. We learned this important lesson through our own mistakes not too long ago, when an AOL employee wrongly revealed the screen name of one of our members to the government.

Recognizing the importance of this issue, AOL has taken a number of steps to create an environment where our members can be certain that their personal information and their choices regarding the use of that information are being respected: from creating and implementing our own privacy policies and educating our members about them, to promoting best practices among our business partners, to engag-

ing in industry-wide initiatives and enforcement mechanisms that will raise the bar for all companies who do business online.

Although the Internet is growing at a tremendous pace, we are still only at the beginning of the development of this new medium. Industry initiatives are helping to craft the “rules of the road” that will dictate online business practices, and we believe that it is important to see how those rules develop rather than imposing a sweeping regulatory framework on the Internet and e-commerce. Therefore, we hope to continue working with policymakers, consumer groups, and industry colleagues to promote industry-led, market-driven initiatives that will build on the progress we have already made and ensure that individual privacy is protected online.

SETTING AN EXAMPLE

AOL is committed to protecting consumer privacy. Building on the lessons we have learned and the input we have received from our members, we have created privacy policies that clearly explain to our users what information we collect, why we collect it, and how they can exercise choice about the use and disclosure of that information. We update our policies and procedures to respond to changes in technology or consumer demand, but our commitment to core privacy protections remains constant. AOL’s current privacy policy is organized around 8 core principles:

- (1) We do not read your private online communications.
- (2) We do not use any information about where you personally go on AOL or the Web, and we do not give it out to others.
- (3) We do not give out your telephone number, credit card information or screen names, unless you authorize us to do so. And we give you the opportunity to correct your personal contact and billing information at any time.
- (4) We may use information about the kinds of products you buy from AOL to make other marketing offers to you, unless you tell us not to. We do not give out this purchase data to others.
- (5) We give you choices about how AOL uses your personal information.
- (6) We take extra steps to protect the safety and privacy of children.
- (7) We use secure technology, privacy protection controls and restrictions on employee access in order to safeguard your personal information.
- (8) We will keep you informed, clearly and prominently, about what we do with your personal information, and we will advise you if we change our policy.

We give consumers clear choices about how their personal information is used, and we make sure that our users are well informed about what those choices are. For instance, if an AOL subscriber decides that she does not want to receive any targeted marketing notices from us based on his personal information or preferences, he can simply check a box on our service that will let us know not to use his data for this purpose. Because we know this issue is so critically important to our members and users, we make every effort to ensure that our privacy policies are clearly communicated to our customers from the start of their online experience, and we notify our members whenever our policies are changed in any way.

We also make sure that our policies are well understood and properly implemented by our employees. We require all employees to sign and agree to abide by our privacy policy, and we provide our managers with training on how to ensure privacy compliance. We are committed to using state-of-the-art technology to ensure that the choices individuals make about their data online are honored. And, we believe that our commitment to consumer privacy and the means we give our subscribers to exercise their privacy prerogatives gives us a clear and meaningful market advantage in attracting and retaining subscribers.

Finally, we try to keep users informed about the steps they can take to protect their own privacy online. For instance, we emphasize to our members that they must be careful not to give out their personal information unless they specifically know the entity or person with whom they are dealing, and we encourage them to check to see whether the sites they visit on the Web have posted privacy policies.

PROTECTING CHILDREN ONLINE

AOL takes extra steps to protect the safety and privacy of children online. One of our highest priorities has always been to ensure that the children who use our service can enjoy a safe and rewarding online experience, and we believe that privacy is a critical element of children’s online safety.

We have created a special environment just for children—our “Kids Only” area—where extra protections are in place to ensure that our children are in the safest possible environment. In order to safeguard kids’ privacy, AOL does not collect personal information from children without their parents’ knowledge and consent, and we carefully monitor all of the Kids Only chat rooms and message boards to make

sure that a child does not post personal information that could allow a stranger to contact the child offline. Furthermore, through AOL's "Parental Controls," parents are able to protect their children's privacy by setting strict limits on whom their children may send e-mail to and receive e-mail from online.

Because of the unique concerns relating to child safety in the online environment, AOL supported legislation in the 105th Congress to set baseline standards for protecting kids' privacy online. We worked with Senator Bryan, the FTC, and key industry and public interest groups to help bring the Child Online Privacy Protection Act (COPPA) to fruition last year. We believe the enactment of this bill was a major step in the ongoing effort to make the Internet safe for children.

FOSTERING BEST PRACTICES

In addition to adopting and implementing our own policies, AOL is committed to fostering best practices among our business partners and industry colleagues. One of the strongest examples of this effort is our "Certified Merchant" program, through which we work with our business partners to guarantee our members the highest standards of privacy and customer satisfaction when they are within the AOL environment. AOL carefully selects the merchants we allow in the program (currently there are over 150 participants), and requires all participants to adhere to strict consumer protection standards and privacy policies. The Certified Merchant principles are posted clearly in all of our online shopping areas, thereby ensuring that both consumers and merchants have notice of the rules involved and the details of the enforcement mechanisms, which help to foster consumer trust and merchant responsiveness.

Here are the criteria that our merchants have to meet in order to become certified and to display the America Online Seal of Approval (some screen shots that show how these criteria appear to subscribers on our service are attached to this testimony):

1. Post complete details of their Customer Service policies, including: Contact Information, Shipping Information, Returns Policies, and Money-Back Satisfaction Guarantee Information.
2. Receive and respond to e-mails within one business day of receipt.
3. Monitor online store to minimize/eliminate out-of-stock merchandise available.
4. Receive orders electronically to process orders within one business day of receipt.
5. Provide the customer with an order confirmation within one business day of receipt.
6. Deliver all merchandise in professional packaging. All packages should arrive undamaged, well-packed, and neat, barring any shipping disasters.
7. Ship the displayed product at the price displayed without substituting.
8. Agree to adopt privacy policies that comport with AOL's privacy policy.

Through our Certified Merchant program, we commit to our members that they will be satisfied with their online experience, and we have developed a money-back guarantee program to dispel consumer concerns about shopping online and increase consumer trust in this powerful new medium. We believe that these high standards for consumer protection and fair information practices will help bolster consumer confidence and encourage our members to engage in electronic commerce.

HELPING TO PROMOTE INDUSTRY EFFORTS

The online industry as a whole is taking positive steps toward protecting consumer privacy. In fact, to improve industry's commitment to online privacy, AOL joined with other companies and associations last year to form the Online Privacy Alliance (OPA), a group dedicated to promoting privacy online.

As you will hear today, the OPA has worked hard to develop a set of core privacy principles—centered around the key concepts of notice, choice, data security, and access—and its members are committed to posting and implementing privacy policies that embody these principles. Since we began our efforts just a few months ago, the OPA has grown to include more than 85 recognized industry leaders, and industry efforts to protect consumer privacy online have blossomed.

A recent study conducted by Georgetown University Professor Mary Culnan shows that, in a sample drawn from a pool of the 7500 most visited websites, more than 65% of the sites have posted a privacy policy or a statement about their information practices. This number demonstrates a tremendous increase from the number of sites posting policies just one year ago, when the FTC conducted a similar study.

Following closely on the heels of the Georgetown study, the FTC released its report to Congress on the status of the industry's efforts to protect consumers' online privacy and presented testimony before this Subcommittee. Based on the progress

of industry itself, the report concluded that legislation to address online privacy was not appropriate at this time. The FTC credited “responsible elements in the online business community” with accomplishing a great deal in a short amount of time. While the report recognized that more needs to be done to secure consumers’ online privacy, it concluded that industry was best positioned to take the leadership role in those efforts because it is “the least intrusive and most efficient means to ensure fair information practices online, given the rapidly evolving nature of the Internet and computer technology.”

We concur with the FTC’s conclusions; private sector leadership in developing fair information practices online is the right approach to assuring broad privacy protection in that environment, but we also realize that there is still more work to be done. To that end and to build on our success to date, the OPA has renewed its commitment to reach out to businesses nationwide to explain the importance of protecting online privacy and posting meaningful privacy policies.

We believe that the OPA member companies are setting a new standard for online privacy, and that as consumers become more aware of the choices available to them, the marketplace will begin to demand robust privacy policies of all companies that do business online. But we also understand the need for meaningful enforcement of industry standards. That’s why we abide by the OPA requirement to participate in robust enforcement mechanisms through our involvement in the TRUSTe and BBBOnline privacy seal programs. We are key sponsors of both the TRUSTe and BBBOnline privacy seal programs, and have worked closely with industry representatives and members of the academic community to help formulate strict standards for seal eligibility.

THE CHALLENGES AHEAD

It is clear that companies are responding to the increasing marketplace demand for online privacy, and that the tremendous growth of e-commerce reflects positive trends on a variety of consumer protection issues, including privacy. But our work has only just begun. As technology makes it easier for companies to collect and use personal information, the adoption and implementation of robust privacy policies will become even more important.

In part, we believe that technology holds the key to ensuring a safe and secure online environment. As an online service provider, we believe it is critical for us to be able to provide the most sophisticated security technologies to our members so that they can take steps to protect their own privacy online. That’s why we will continue to advocate the widespread availability and use of strong encryption, both in this country and abroad.

The challenges that lie ahead will give us the chance to prove that industry and government can work together to promote online privacy. But ultimately, it is the consumer who will be the judge of whether these efforts are adequate. Because no matter how extraordinary the opportunities for electronic commerce may be, the marketplace will fail if we cannot meet consumers’ demands for privacy protection and gain their trust.

LEGISLATIVE PROPOSALS

The focus of today’s hearing is legislation designed to extend the privacy provisions in COPPA to adults—the Online Privacy Protection Act of 1999, S. 809—sponsored by Chairman Burns and Senator Wyden. AOL urges the Committee to proceed with great caution in considering this or any legislation that would extend regulation of the Internet beyond what is currently in force. Not only is generally privacy regulation premature, but we are concerned about unanticipated consequences that could affect the growth of electronic commerce or otherwise harm consumers and/or the industry.

As the Georgetown study showed and the FTC report confirmed, industry led efforts have resulted in a tremendous increase in website adoption of privacy policies in a very short amount of time. And, as AOL has testified, industry is committed to continuing those efforts to achieve even greater progress in the future. Consequently, it is premature to consider legislation to address any gaps in self-regulation until it becomes apparent where such gaps would be. As the FTC report concluded, industry-led efforts to address online privacy are “the least intrusive and most efficient means” to accomplish the important public policy objective of creating a secure online environment for consumers. Private sector efforts should be given an opportunity to mature fully before Congress considers seriously whether further privacy legislation is necessary or prudent.

This is not to say that Congress should be any less vigilant in tracking industries’ progress and identifying areas where legislation is appropriate. For example, as

noted previously, AOL supported COPPA because of the unique concerns related to child safety in the online environment. However, even that legislation, which was carefully crafted and widely vetted, is raising challenging interpretation and implementation issues for the FTC and for the industry. Just last week, the Commission convened a special workshop in an attempt to get a better understanding of the myriad issues involved in obtaining verifiable parental consent, including whether the federal regulation proposed would discourage Internet start ups from offering content designed for children.

With respect to the specifics of S. 809, AOL urges the Committee to consider focusing not on a regulatory framework for online privacy, but rather on strengthening the FTC's enforcement authority to prevent fraudulent business practices. In that way, the "bad guys" can be stopped and the "good guys" can continue to serve consumers with innovative services and products. Our research shows that consumers are most interested in an honest exchange. They see the benefit of the services they receive online, but want to ensure that they know who will have access to any information they give out and how it will be used.

SUMMARY

We at AOL are committed to doing our part to protecting personal privacy online. Our customers demand it, and our business requires it—but most importantly, the growth and success of the online medium depend on it. We appreciate the opportunity to discuss these important issues before the Committee, and look forward to continuing to work with you on other matters relating to the Internet and electronic commerce.

Senator BURNS. Thank you very much. Now we will hear from Ms. Deirdre Mulligan, who is staff counsel, Center for Democracy and Technology.

STATEMENT OF DEIRDRE MULLIGAN, STAFF COUNSEL, CENTER FOR DEMOCRACY AND TECHNOLOGY

Ms. MULLIGAN. Thank you so much for the opportunity to be here. I want to first thank the chairman and Senator Wyden and Senator Bryan for their leadership on the privacy issue and also for your work on encryption.

As you have heard from everyone so far this morning, and my guess is you will continue to hear today, there is a fair amount of consensus in this room, and I think what I have heard from the members of this subcommittee, there has been an agreement that consumers are concerned about their privacy. Eighty-seven percent of consumers have registered concern—a very high percentage of consumers. And I think Senator Wyden's earlier comments about very informed consumers, such as chief information officers, are incredibly reluctant to participate in all of the benefits that this new technology has to offer for fear of loss of personal privacy.

You have heard widespread agreement that abiding by fair information practices, or, I would at least say, a narrower subset of fair information practices, that have been offered by the Federal Trade Commission, would substantially address consumers' concerns and help to establish a framework that will both promote privacy and enable widespread use of electronic commerce.

You have also heard agreement that it is in businesses' enlightened self-interest to proceed in this direction. Yet we have also noted that despite some very, very commendable efforts, right now we have a less than stellar record on actually seeing a widespread and ubiquitous enforcement of those policies in the commercial marketplace.

We will also agree that business practices, best business practices, need to continue to move forward, and that the private sector

does have a role to play in raising the benchmark, and that self-regulatory programs will need to be a part of this very free-wheeling and, as we heard, 3.6 million commercial Web sites and growing by 10 percent on a daily basis, we need as many cops on the beat as possible.

So, where will we disagree?

I think, as Senator Wyden pointed out, and Senator Burns, and the discussion around S. 809 indicates, the agreement is not about where we should go; the agreement is primarily about how best to get there.

I would like to submit for the record a report that CDT is releasing today. And it is called "Behind the Numbers: Privacy Practices on the Web." And what we tried to do is actually say we have some statistics, from the Georgetown Internet Privacy Policy Survey, the Online Privacy Alliance's Survey, from the Federal Trade Commission survey last year, that give us some indication of where practices are going in the online world.

What we have found is that while there has been some progress, that many of the most deeply held concerns of consumers remain unaddressed. For example, 87 percent of individuals stated a concern with their privacy online. But a third of the highly trafficked Web sites—this is not the 3.6 million, this is the 7,500 highly trafficked Web sites—remain silent on the issue of privacy altogether. Ninety-one percent of Internet users and 96 percent of those engaged in e-commerce want to know what personal information is collected and used. But, again, less than 50 percent of these frequently trafficked Web sites are telling consumers this critical information that they need to make informed choices.

Forty percent of business Web sites are not allowing individuals to exercise even a very limited right to object to companies re-contacting them. This was a critical concern. An overwhelming majority of individuals, as people have identified, their top concern is their ability to control the use of their information. And while we would suggest that an opt out, particularly when you are talking about financial records, medical records, which are provided on the Web—individuals are engaging in lots of varied interactions on the Web—an opt out model is clearly not what individuals think is appropriate when they talk about consent.

The question is, how do we move forward?

Part of our survey that I would like to offer for the record looked at the self-regulatory enforcement programs. And there is some good news. TRUSTe, BBBOnline and WebTrust, which are the three that we looked at, are in fact raising the standards for what business practices should be, as self-regulatory programs should do.

Right now, unfortunately, I think that there is the opportunity for an enormous amount of consumer confusion. Two of the self-regulatory programs are actually in the process of changing their standards. And so, right now, a mark may mean that a company is telling consumers what they do. It may mean that it is actually adhering to a higher set of fair information practices. But the main lesson to consumers is that even where there is a trust mark, you have to read the fine print, and that caution is certainly wise.

On the down side, less than 8.5 percent of even the 7,500 highly trafficked Web sites are using these programs. And I would sug-

gest, when you look at the 3.6 million Web sites, that are growing by 275,000 a day, that 900 Web sites participating in self-regulatory enforcement programs is not going to provide the kind of ubiquitous, enforceable privacy protections that the FTC has requested and that I think consumers both demand and deserve.

For that reason, I think that S. 809 serves as a good starting point for a discussion about how to move forward on protecting privacy. I think that as Commissioner Swindle said earlier, the third of the Web sites that are not posting privacy policies, are they necessarily bad actors? Perhaps not. Do they necessarily need some guidance? I would suggest yes.

Is there a reason why individual companies are not choosing to participate in self-regulatory enforcement programs? I believe there may be several—one of which may be cost. The fact that there is a Federal baseline, with a Federal enforcement mechanism, is something that in fact can continue to maintain the very low barriers to entry that we have in this marketplace.

So, in moving forward, I look forward to working with the Federal Trade Commission, members of both industry and the public interest sector, and members of this committee to figure out how to craft an appropriate framework that relies on self-regulation, legislation and technology to address individuals privacy concerns.

Thank you.

[The prepared statement of Ms. Mulligan follows:]

PREPARED STATEMENT OF DEIRDRE MULLIGAN, STAFF COUNSEL,
CENTER FOR DEMOCRACY AND TECHNOLOGY

I. OVERVIEW

The Center for Democracy and Technology (CDT) is pleased to have this opportunity to testify about privacy in the online environment. CDT is a non-profit, public interest organization dedicated to developing and implementing public policies to protect and advance civil liberties and democratic values on the Internet. One of our core goals is to enhance privacy protections for individuals in the development and use of new communications technologies. We thank the Chairman and Senators Wyden and Hollings for holding this hearing and for their commitment to seeking policies that support both civil liberties and a vibrant Internet.

CDT wishes to emphasize three points this morning:

- The Internet presents new challenges and opportunities for the protection of privacy. Our policies must be grounded in an understanding of the medium's unique attributes and its unique potential to promote democratic values.

- Privacy is a complex value. In the context of this discussion, we believe Congress should focus on ensuring that individuals' long-held expectations of autonomy, fairness, and confidentiality are respected as daily activities move online. These expectations exist vis-a-vis both the public and the private sectors.

By autonomy, we mean the individual's ability to browse, seek out information, and engage in a range of activities without being monitored and identified.

Fairness requires policies that provide individuals with control over information that they provide to the government and the private sector. The concept of fairness is embodied in the Code of Fair Information Practices¹—long-accepted principles

¹The Code of Fair Information Practices as stated in the Secretary's Advisory Comm. on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens, U.S. Dept. of Health, Education and Welfare, July 1973:

There must be no personal data record-keeping systems whose very existence is secret.

There must be a way for an individual to find out what information about him is in a record and how it is used.

There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

There must be a way for the individual to correct or amend a record of identifiable information about him.

specifying that individuals should be able to “determine for themselves when, how, and to what extent information about them is shared.”² The Code also requires that those who collect and use personal information do so in a manner that respects individuals’ privacy interests. Self-regulatory efforts designed for the online environment are gradually moving closer to the standards for privacy protection set out in the Code of Fair Information Practices. However, legislation, as well as robust self-regulation, is both inevitable and necessary to ensure privacy protection is the rule rather than the exception on the Internet. The Children’s Online Privacy Protection Act, which originated in the full Committee, enacted last October provides a model for establishing such a legal framework. The Online Privacy Protection Act of 1999 (S. 809), with modifications, would provide a similar framework for protecting adult privacy and establishing the authority of the Federal Trade Commission to punish back actors.

In terms of confidentiality, we need a strong Fourth Amendment in cyberspace. But confidentiality protections—both technical and legal—are growing increasingly porous as technology changes and more information resides outside of the home on networks. It is time to update and strengthen the Electronic Communications Privacy Act. Further, our laws protecting privacy must be extended to take account of the global nature of the medium. Finally, to ensure that citizens and businesses have the ability to protect their sensitive information and communications, the government must change its policy course on encryption.

- Preserving these core elements of privacy on the Internet requires a thoughtful, multi-faceted approach combining self-regulatory, technological, and legislative components.

II. WHAT MAKES THE INTERNET DIFFERENT?

CDT focuses much of its work on the Internet because we believe that it, more than any other medium, has characteristics—architectural, economic, and social—that are uniquely supportive of democratic values. Because of its decentralized, open, and interactive nature, the Internet is the first electronic medium to allow every user to “publish” and engage in commerce. Users can reach and create communities of interest despite geographic, social, and political barriers. As the World

Any organization creating, maintaining, using, or disseminating records of identifiable personal data must reliability of the data for their intended use and must take precautions to prevent misuse of the data. *Id.* at xx

The Code of Fair Information Practices as stated in the OECD guidelines on the Protection of Privacy and Transborder Flows of Personal Data <http://www.oecd.org/dsti/sti/ii/secur/prod/PRIV-EN.HTM>

1. Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data quality: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose specification: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use limitation: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the ‘purpose specification’ except: (a) with the consent of the data subject; or (b) by the authority of law.

5. Security safeguards: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. Openness: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual participation: An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him:

- within a reasonable time;
- at a charge, if any, that is not excessive;
- in a reasonable manner; and,

- in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and, (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified completed or amended.

8. Accountability: A data controller should be accountable for complying with measures which give effect to the principles stated above.

²Alan Westin. *Privacy and Freedom* (New York: Atheneum, 1967), 7.

Wide Web grows to fully support voice, data, and video, it will become in many respects a virtual “face-to-face” social and political milieu.

But while the First Amendment potential of the Internet is clear, and recognized by the Supreme Court, the impact of the Internet on individual privacy is less certain. Will the online environment erode individual privacy-building in national identifiers, tracking devices, and limits on autonomy? Or will it breathe new life into privacy-providing protections for individuals’ long held expectations of privacy? The Internet poses both challenges and opportunities to protecting privacy.

The Internet accelerates the trend toward increased information collection that is already evident in our offline world. The trail of transactional data left behind as individuals use the Internet is a rich source of information about their habits of association, speech, and commerce. When aggregated, these digital fingerprints reveal a great deal about an individual’s life. The global flow of personal communications and information coupled with the Internet’s distributed architecture presents challenges for the protection of privacy. However, Anonymizers, anonymous remailers, and other privacy-enhancing tools allow individuals to create zones of privacy—limiting who knows what about them and protecting their sensitive communications from prying eyes. Computer code and products are becoming increasingly critical to the protection of privacy in this distributed environment. With privacy-enhancing tools users will be empowered to control their personal information in new ways.

As we move swiftly toward a world of electronic democracy, electronic commerce and indeed electronic living, it is critical to construct a framework of privacy protection that fits with the unique opportunities and risks posed by the Internet. But as Congress has discovered in its attempts to regulate speech, this medium deserves its own analysis. Laws developed to protect interests in other media should not be blindly imported. To create rules that map onto the Internet, we must fully understand the characteristics of the Internet and their implications for privacy protection. We must also have a shared understanding of what we mean by privacy. Finally we must assess how to best use the various tools we have for implementing policy—law, computer code, industry practices, and public education—to achieve the protections we seek.

THE EROSION OF PRIVACY AND THE PATH TOWARDS ITS RESTORATION

There are several core “privacy expectations” that individuals have long held vis-a-vis both the government and the private sector, the protection of which should carry over to interactions on the Internet. Surveys of Internet users, and would-be Internet users, reveal a high level of concern with threats to privacy online. Surveys suggest that concern over privacy is keeping individuals off the Internet³, retarding the growth of e-commerce⁴, and leading individuals to engage in privacy-protective behaviors such as providing false information.⁵ A recent survey of Internet users found that 87% are concerned about threats to their personal privacy.⁶

The remainder of our testimony will discuss the three critical privacy expectations of autonomy, fairness, and confidentiality, explore the changes in technology and policies that threaten them, and finally outline a plan for their restoration.

The Expectation of Autonomy

Why is it at risk?

Imagine walking through a mall where every store, unbeknownst to you, placed a sign on your back. The signs tell every other store you visit exactly where you have been, what you looked at, and what you purchased. Something very close to this is possible on the Internet.

When individuals surf the World Wide Web, they have a general expectation of anonymity, more so than in the physical world where an individual may be observed by others. As documented in several surveys, individuals value their anonymity and will take steps, such as providing false information and refusing to register, to protect it.⁷ Online, individuals often believe that if they have not affirmatively disclosed

³A 1998 Business Week Survey found that privacy was the number one reason individuals are choosing to stay off the Internet, coming in well ahead of cost, concerns with complicated technology, and concerns with unsolicited commercial email. Business Week, March 16, 1998.

⁴A TRUSTe and Boston Consulting Group survey conducted in 1997 found that privacy concerns were leading users to limit their engagement in electronic commerce.

⁵Id. and see footnote 6.

⁶Beyond Concern: Understanding Net Users Attitudes About Online Privacy, AT&T, 1999.

⁷The 8th annual poll of the Graphics, Visualization, and Usability Center at the Georgia Institute of Technology found that in order to protect their privacy, significant numbers of people falsify information online. Particularly, users report regularly falsifying registration information. The most common reason for not registering is the lack of a statement about how the informa-

information about themselves, then no one knows who they are or what they are doing. But, contrary to this belief, the Internet generates an elaborate trail of data detailing every stop a person makes. The individual's employer may capture this data trail if she logs on at work, and it is captured by the Web sites the individual visits. This transactional or click stream data can provide a 'profile' of an individual's online life.

Two recent examples highlight the manner in which individuals' expectation of autonomy is increasingly challenged in the online environment. (1) The introduction of the Pentium III processor equipped with a unique identifier (Processor Serial Number) threatens to greatly expand the ability of Web sites to surreptitiously track and monitor online behavior. The PSN could become something akin to the Social Security Number of the online world—a number tied inextricably to the individual and used to validate one's identity throughout a range of interactions with the government and the private sector. (2) The Child Online Protection Act (COPA), passed in October, requires Web sites to prohibit minors' access to material considered "harmful to minors." Today, when an individual walks into a convenience store to purchase an adult magazine, they may be asked to show some identification to prove their age. Under the COPA, an individual will be asked not only to show their identification, but also to leave a record of it and their purchase with the online store. Such systems will create records of individuals' First Amendment activities, thereby conditioning adult access to constitutionally protected speech on a disclosure of identity. This poses a Faustian choice to individuals seeking access to information—protect privacy and lose access or exercise First Amendment freedoms and forego privacy.

The Path to Individual Autonomy Online

While the global, distributed environment of the Internet raises challenges to our traditional methods of implementing policy, the specifications, standards, and technical protocols that support the operation of the Internet offer a new way to implement policy decisions. In the area of autonomy, focusing on standards and applications is crucial. By building systems that respect individuals varied needs for identification, pseudonymity, and anonymity—building a digital wallet with cash, credit cards, a metro fare card, and a driver's license—will help build an online environment that promotes autonomy. By building privacy into the architecture of the Internet, we have the opportunity to advance public policies in a manner that scales with the global and decentralized character of the network. As Larry Lessig repeatedly reminds us, "(computer) code is law."

Accordingly, we must promote specifications, standards and products that protect privacy. A privacy-enhancing architecture must incorporate, in its design and function, individuals' expectations of privacy. For example, a privacy-friendly architecture would provide individuals the ability to "walk" through the digital world, browse, and even purchase without disclosing information about their identity, thereby preserving their autonomy. Of course, it would also provide individuals the opportunity to create relationships that are identifiable—or at least authenticated—for engaging in activities such as banking. This would be coupled with policies that allow individuals to control when, how, and to whom personal data collected during interactions is used or disclosed.

While there is much work to be done in designing a privacy-enhancing architecture, some substantial steps toward privacy protection have occurred. Positive steps to leverage the power of technology to protect privacy can be witnessed in tools like the Anonymizer, Crowds, and Onion Routing, which shield individuals' identity during online interactions, and encryption tools such as Pretty Good Privacy that allow individuals to protect their private communications during transit. Coupled with rules such as those found in the Government Paperwork Elimination Act of 1998, which established privacy protections governing personal information collected when the public uses electronic signature systems,⁸ technology may evolve in ways that support individuals' interest in autonomy.

tion will be used. In addition, the GW study showed that users would rather not access a site than reveal information. (1998)

The survey *Beyond Concern: Understanding Net Users Attitudes About Online Privacy* found that individuals were reluctant to provide identifying information such as credit card numbers but were more willing to provide information that did not identify them. AT&T (1999)

⁸ Many such systems gather sensitive information in the course of providing and guaranteeing an electronic signature. The law prohibits companies that collect such information from using or disclosing it without the permission of the person involved. Authored by Senators Leahy and Abraham, this marks the first attempt to craft a legislative approach to dealing with the potential erosion of privacy created by electronic signature use.

*The Expectation of Fairness and Control Over Personal Information**Who controls the data?*

When individuals provide information to a doctor, a merchant, or a bank, they expect that those professionals/companies will collect only information necessary to perform the service and use it only for that purpose. The doctor will use it to tend to their health, the merchant will use it to process the bill and ship the product, and the bank will use it to manage their account—end of story. Unfortunately, current practices, both offline and online, foil this expectation of privacy. Much of the concern with privacy in electronic commerce stems from a lack of privacy rules in various sectors of the economy, such as financial and health, that handle a treasure trove of sensitive information on individuals.

Whether it is medical information, or a record of a book purchased at the bookstore, or information left behind during a Web site visit, information is routinely collected without the individual's knowledge and used for a variety of other purposes without the individual's knowledge—let alone consent.

Focusing on the online environment, we now have information from two studies assessing the state of privacy notices on the World Wide Web. Last June, the Federal Trade Commission's "Privacy Online: A Report to Congress" found that despite increased pressure, businesses operating online continued to collect personal information without providing even a minimum of consumer protection. The report looked only at whether Web sites provided users with notice about how their data was to be used; there was no discussion of whether the stated privacy policies provided adequate protection. The survey found that, while 92% of the sites surveyed were collecting personally identifiable information, only 14% had some kind of disclosure of what they were doing with personal data.

The newly released Georgetown Internet Privacy Policy Survey provides new data. The Survey was designed to provide an update on the state of privacy policies on the World Wide Web. The study shows that definite progress has been made in making many more Web sites privacy-sensitive, but substantive privacy protections are still far from ubiquitous on the World Wide Web. While more Web sites are mentioning privacy, only 9.5% provide the types of notices required by the Online Privacy Alliance, the Better Business Bureau and TRUSTe. Indeed, fair information practices on the Web appear to remain the exception, not the rule.

The Georgetown Survey shows that, spurred by surveys documenting consumer concern and anxiety, and the work of individual companies⁹ and industry self-regulatory entities such as TRUSTe, the Online Privacy Alliance, and the Better Business Bureau, an increased number of Web sites are providing consumers with some information about what personal information is collected (44%), and how that information will be used (52%). Companies posting fuller information about their data handling¹⁰ are more likely to make them accessible to consumers. Many have a link to such statements from the home page (79.7%).¹¹

However, on important issues such as access to personal information and the ability to correct inaccurate information, the Georgetown Survey shows that only 22% and 18% respectively of these highly trafficked Web sites provide consumers with notice. On the important issue of providing individuals with the capacity to control the use and disclosure of personal information, the survey finds that 39.5% of these busy Web sites say that consumers can make some decision about whether they are re-contacted for marketing purposes—most likely an "opt-out"—and fewer still, 25%, say they provide consumers with some control over the disclosure of data to third parties.¹²

Overall, the Georgetown survey reveals that, at over 90% of the most frequently trafficked Web sites,¹³ consumers are not being adequately informed about how

⁹ For example, IBM recently stated that it would limit its advertising to Web sites that post privacy notices.

¹⁰ The report calls these "privacy policies" as compared to "information practice statements." "Privacy policies" are a more comprehensive description of a site's practices that are located in a single place and accessible through an icon or hyperlink. A site may have a "privacy policy" by this definition but still not have a privacy policy that meets the elements set out by the FTC or various industry self-regulatory initiatives for an adequate privacy policy.

¹¹ In response to the question, "Is a Privacy Policy Notice easy to find?" surfers in the 1998 survey answered yes for approximately 1.2% of Web sites. FTC Report, Appendix C Q19.

¹² This number is generated using the data from Q32 (number of sites that say they give consumers choice about having collected information disclosed to outside third parties)—64—and dividing it by 256 (the total survey sample (364) minus the number of sites that affirmatively state they do not disclose data to third-parties (Q29A) (69) and the number of sites that affirmatively state that data is only disclosed in the aggregate (Q30) (39)).

¹³ Only 9.5% of the most frequently visited Web sites and 14.7% of those that collect information had privacy policies containing critical information called for by the FTC, the Administra-

their personal information is handled.¹⁴ At the same time the survey found that over 90% of these same busy consumer-oriented Web sites are collecting personal information.¹⁵ In fact, the survey revealed an increase in the number of Web sites collecting sensitive information such as credit card numbers (up 20%), names (up 13.3%), and even Social Security Numbers (up 1.7%).

Thus, while many companies appear to be making an effort to address some privacy concerns, the results from the consumer perspective appear to be a quilt of complex and inconsistent statements. The number of sites that provide consumers with the types of notices required by the Online Privacy Alliance, the Better Business Bureau and TRUSTe, and called for by the Federal Trade Commission and the Administration, is still relatively small (9.5%).

The posting of privacy notices is not just a private sector issue. In a recent CDT study of federal agency Web sites, we found that just over one-third of federal agencies had a "privacy notice" link from the agency's home page. Eight other sites had privacy policies that could be found after following a link or two and on 22 of the sites surveyed we could not find a privacy policy at all.

The lack of widespread adherence to Fair Information Practices is undermining consumer confidence. A recent survey by the National Consumers League found that the majority of online users are not comfortable providing credit card (73%), financial (73%), or personal information (70%) to businesses online.¹⁶ Due to privacy concerns 42% of those who use the Internet are using it solely to gather information, while a smaller 24% actually venture to purchase goods online.¹⁷ A second study found that 58% of consumers do not consider financial transactions online to be safe, and 77% do not believe it is safe to provide a credit card number through a computer.¹⁸ Privacy has been rightly identified by the Federal Trade Commission, Congress, the business community, and advocacy organizations as a critical consumer protection issue in e-commerce.

Establish Rules That Give Individuals Control Over Personal Information During Commercial Interactions

We must adopt enforceable standards, both self-regulatory and legislative, to ensure that information provided for one purpose is not used or redisclosed for other purposes without the individual's consent. All such efforts should focus on the Code of Fair Information Practices developed by the Department of Health, Education and Welfare in 1973. The challenge of implementing privacy practices on the Internet is ensuring that they build upon the medium's real-time and interactive nature to foster privacy and that they do not unintentionally impede other beneficial aspects of the medium. Implementing privacy protections on the global and decentralized Internet is a complex task that will require new thinking and innovative approaches.

The Georgetown Survey supports our belief that a combination of means—self-regulation, technology, and legislation—are required to provide privacy protections on the Internet. The study, as discussed above, shows that some progress has been made in making many more Web sites privacy sensitive, but substantive privacy protections are still far from ubiquitous on the World Wide Web. Because many Web sites need baseline policy guidance and because self-enforcement mechanisms, while emerging, may not always provide a viable remedy, we believe that legislation is both inevitable and necessary to ensure consumers' privacy on the Internet.

To achieve real privacy on the Internet, we will need more than better numbers, redoubled efforts by industry, or a legislative mantra. We will need a good-faith concerted effort by industry, consumer and privacy advocates, and policymakers to develop real and substantive answers to a number of difficult policy issues involving the scope of identifiable information, the workings of consent and access mechanisms, and the structure of effective remedies that protect privacy without adversely affecting the openness and vitality of the Internet.

As the Federal Trade Commission's rulemaking under the Children's Online Privacy Protection Act and industry's various efforts at self-regulation show, these issues are not easy. But armed with the findings of the Georgetown Internet Privacy Policy Survey, we believe interested parties are in a position to move forward on a three pronged approach—expanded self-regulation, work to develop and deploy

tion, and required by the Online Privacy Alliance, Truste and the BBB Online, about notice; choice; access; security; and contact information.

¹⁴ Last years survey found approximately 2% of Web sites that collected data, and less than 1% of all Web sites, had adequate notices.

¹⁵ 92.9% are collecting some type of personal information.

¹⁶ Consumers and the 21st Century, National Consumers League (1999).

¹⁷ Id.

¹⁸ National Technology Readiness Survey, conducted by Rockridge Associates (1999).

privacy-enhancing technologies such as P3P, and legislation—all require a serious dialogue on policy and practice options for resolving difficult issues in this promising medium.

In its testimony last July, the Federal Trade Commission stated that, “ * * * unless industry can demonstrate that it has developed and implemented broad-based and effective self-regulatory programs by the end of this year, additional governmental authority in this area would be appropriate and necessary.”¹⁹ Despite the considerable effort of Congress, the Federal Trade Commission, the Administration and industry to encourage and facilitate an effective self-regulatory system to protect consumer privacy, based on the survey results we do not believe that one has yet emerged. Like Commissioner Anthony, we believe that industry leadership and self-regulatory programs are a critical component of a privacy framework for the Internet, but that legislation is also necessary to establish a baseline and ensure consumers are protected from bad actors.

Last year, the Federal Trade Commission offered a legislative outline that embodied a framework, similar to the one we suggest, building upon the strengths of both the self-regulatory and regulatory processes. This year several bills have been introduced on a wide range of privacy issues.²⁰ The Online Privacy Protection Act²¹ introduced by Senators Burns and Wyden is substantially similar to the model recommended by the Federal Trade Commission last year. (Specific comments on the Online Privacy Protection Act can be found in subsection 3 below.)

Historically, for privacy legislation to be successful, it must garner the support of at least a section of the industry. To do so, it generally must build upon the work of some industry members typically binding bad actors to the rules being followed by industry leaders—or be critically tied to the viability of a business service or product as with the Video Privacy Protection Act and the Electronic Communications Privacy Act. Several companies have staked out leadership positions on the issue of online privacy and several self-regulatory programs have formed to drive industry best practices online. Numerous surveys have documented that consumers are concerned about their privacy in e-commerce.

In addition to work on policies, there is important activity in the technical community on how to develop the tools necessary to implement fair information practices on the World Wide Web. The World Wide Web Consortium’s Platform for Privacy Preferences (“P3P”) is a promising development. The P3P specification will allow individuals to query Web sites for their policies on handling personal information and to allow Web sites to easily respond. While P3P does not drive the specific practices, it is a standard designed to promote openness about information practices, to encourage Web sites to post privacy policies and to provide individuals with a simple, automated method to make informed decisions. Through settings on their Web browsers, or through other software programs, users will be able to exercise greater control over the use of their personal information. Regardless of how policies are established, an Internet-centric method of communicating about privacy is part of the solution.

As Congress moves forward this year, we look forward to working with you and all interested parties to ensure that fair information practices are incorporated into business practices on the World Wide Web. Both legislation and self-regulation are only as good as the substantive policies they embody. As we said at the start, crafting meaningful privacy protections that map onto the Internet requires us to resolve several critical issues. While consensus exists around at least four general principles (a subset of the Code of Fair Information Practices)—notice of data practices; individual control over the secondary use of data; access to personal information; and, security for data—the specifics of their implementation and the remedies for their violation must be explored. We must wrestle with difficult questions: When is information identifiable? How is it accessed? How do we create meaningful and proportionate remedies that address the disclosure of sensitive medical information as well as the disclosure of inaccurate marketing data? For the policy process to suc-

¹⁹Last years survey found approximately 2 percent of Web sites that collected data, and less than 1 percent of all Web sites, had adequate notices. *Privacy Online: A Report to Congress*, Federal Trade Commission, June 1998.

²⁰Electronic Rights for the Twenty-First Century Act of 1999 (E-RIGHTS) (S. 854), introduced on April 21, 1999 by Senator Leahy (D-VT). The Online Privacy Protection Act of 1999 (S. 809), introduced on April 15, 1999, by Senators Burns (R-MT) and Wyden (D-OR). Internet Growth and Development Act of 1999 (H.R. 1685), introduced on May 5, 1999 by Representatives Boucher (D-VA) and Goodlatte (R-VA). Consumer Internet Privacy Protection Act of 1999 (H.R. 313), introduced on January 6, 1999, by Representative Vento (D-MN). We anticipate additional proposals from Senators Kohl, Torricelli, DeWine, and Hatch, and Representative Markey.

²¹The Online Privacy Protection Act of 1999 (S. 809), introduced on April 15, 1999, by Senators Burns (R-MT) and Wyden (D-OR).

cessfully move forward these hard issues must be more fully resolved. We would welcome the opportunity to work with Senators Burns and Wyden, and other members of this committee, to explore these issues and develop a framework for privacy protection in the online environment. The Online Privacy Protection Act could serve as a starting point for this discussion. The leadership of Internet-savvy members of this Committee and others will be critical as we seek to provide workable and effective privacy protections for the Internet.

3. Preliminary Comments on the Online Privacy Protection Act (S. 809) and suggested changes

The Online Privacy Protection Act is closely modeled on the Children's Online Privacy Protection Act enacted last year. It establishes baseline practices for commercial Web sites handling personal information and provides the Federal Trade Commission with authority to enforce violations of the Act.

Legislation to protect privacy should be based on the Code of Fair Information Practices which has served as a model for privacy legislation and self-regulatory codes in the United States and across the globe for 25 years.

The Code of Fair Information Practices requires that businesses collecting personal information (recordkeepers):

Be publicly identified and provide a description of the purpose and uses they make of personal information.

Limit the personal information they collect to what is necessary to support the purpose of collection. Personal information must be collected by lawful and fair means and, where appropriate, with the knowledge and consent of the individual.

Limit the use and disclosure of personal information to the purpose for which it was collected, unless the individual has granted consent.

Ensure that personal information collected is relevant to the purpose of collection, accurate, timely, and complete.

Institute reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification and disclosure.

Be accountable for complying with fair information practices.

The Code of Fair Information Practices says that individuals should have the right to:

Access personal information and to correct or remove data that is not timely, accurate, relevant, or complete; and, to

Control the use of personal information. Personal information provided to a business may not be used or disclosed for other purposes without the consent of the individual or other legal authority.

To bring the Online Privacy Protection Act (S. 809) in line with the Code of Fair Information Practices we recommend the following changes.

Section 2(b)(1)

Individual Control

To ensure that individuals are able to control the use of their personal information, Section 2(b)(1) (A)(ii) should require Web sites to gain individuals consent to the use and disclosure of personal information for purposes unrelated to the purpose for which it was obtained. The range of personal information that will be exchanged on Web sites runs from the highly sensitive—financial and health—to contact information such as email and address. Surveys indicate that individuals desire control over their personal information: consent is the surest method of providing consumers with this control. On the Internet we believe that the distinction between “opt-out” and “opt-in” may become less important as technology enables individuals to exercise control over how, when, for what purposes, and under what conditions they disclose personal information.

The bill summary suggests that the intent of the proposal is to provide individuals with the ability to “opt-out” of having their information used and disclosed. However, as currently drafted this section does not require Web sites to gain the individual's consent, nor does it provide an “opt-out” for the collection or use of information—it requires an “opt-out” be provided where information will be disclosed to others. In addition, section (2) of this provision could be read to allow Web sites to forego offering individuals even an opt-out if in the notice they tell individuals that they disclose information.

Access and Correction

To ensure that individuals are able to review and correct personal information about themselves, section (B)(i) should be amended to require Web sites to provide individuals with access to all personal information regardless of whether it is used internally, or sold or transferred to other companies.

*Section 2(b)(2)**Limits on Disclosure*

We have questions about the purpose of this section. However, at this time, we recommend eliminating subsections (A) and (B) and amending (C) by changing the word “permitted” to “required.” Thus the provision would allow a Web site to disclose personal information where “required under other provisions of law.”

*Section 2(b)(3)**Limits on Access*

We have questions about the purpose of this section. However, at this time, we recommend eliminating subsections (A), (B) and (E). Section (C) should be rewritten to limit access to information that is trade secret.

Additional comments

The scope of the bill is information collected online—this means that information collected by Web sites from other sources is not governed by the bill. It is unclear whether consumers, and businesses, distinguish between interactions conducted online and offline with the same entity. As the Committee moves forward, it should consider whether the online/offline distinction is meaningful to consumers and the business community.

Several issues have surfaced during the Federal Trade Commission’s Rulemaking under the Children’s Online Privacy Protection Act that would benefit from additional consideration by this Committee. They include: what does it mean to “collect” information in the online context; when is information personally identifiable; and, what does it mean to “contact” an individual online. In addition, the Children’s Online Privacy Protection Act, and the proposed Online Privacy Protection Act, give enforcement authority to the Federal Trade Commission while other privacy statutes tend to provide individuals with private rights of actions to address grievances. Arguments can be made in favor and against each model of oversight and enforcement: exploring the effectiveness of each (or a combination thereof) would be useful in crafting meaningful remedies for individuals and successful oversight mechanisms.

C. THE EXPECTATION OF CONFIDENTIALITY

1. Who has access to records in cyberspace?

When individuals send email they expect that only the intended recipient will read it. In passing the Electronic Communications Privacy Act in 1986, Congress reaffirmed this expectation. Unfortunately, it is once again in danger.

While United States law provides email the same legal protection as a first class letter, the technology leaves unencrypted email as vulnerable as a postcard. Compared to a letter, an email message is handled by many independent entities and travels in a relatively unpredictable and unregulated environment. To further complicate matters, the email message may be routed, depending upon traffic patterns, overseas and back, even if it is a purely domestic communication. While the message may effortlessly flow from nation to nation, the privacy protections are likely to stop at the border.

Email is just one example. Today our diaries, medical records, and confidential documents are more likely to be out in the network than stored in our homes. As our wallets become “e-wallets” housed somewhere out on the Internet rather than in our back-pockets, the confidentiality of our personal information is at risk. The advent of online datebooks, and products such as Novell’s “Digital Me”, and sites such as Wellmed.com²² which invite individuals to take advantage of the convenience of the Internet to manage their lives, financial information, and even medical records raise increasingly complex privacy questions. While the real “me” has Fourth and Fifth Amendment protections from the government, the “Digital Me” is increasingly naked in cyberspace.

2. Protecting the Privacy of Communications and Information

Increasingly, our most important records are not “papers” in our “houses” but “bytes” stored electronically at distant “virtual” locations for indefinite periods of

²² WellMed.com is a proprietary Online Health Management System which works by collecting personal health information from individuals, analyzing that information to develop unique health profiles which are used for a variety of purposes. One service is HealthNow!—“an online personal health record enabling secure, confidential, and private storage, management, and maintenance of health information by individuals and their families. HealthNow affords easy access of medical records from one central location anytime and anywhere the need arises.”

time and held by third parties. The Internet, and digital technology generally, accelerate the collection of information about individuals' actions and communications. Our communications, rather than disappearing, are captured and stored on servers controlled by third parties. Daily interactions such as our choice of articles at a news Web site, our search and purchase of an airline ticket, and our use of an on-line date book, such as Yahoo's calendar, leave detailed information in the hands of third-parties. With the rise of networking and the reduction of physical boundaries for privacy, we must ensure that privacy protections apply regardless of where information is stored.

Under our existing law, there are now essentially four legal regimes for access to electronic data: (1) the traditional Fourth Amendment standard for records stored on an individual's hard drive or floppy disks; (2) the Title III-Electronic Communications Privacy Act standard for records in transmission; (3) the standard for business records held by third parties, available on a mere subpoena to the third party with no notice to the individual subject of the record; and (4) a statutory standard allowing subpoena access and delayed notice for records stored on a remote server, such as the diary of a student stored on a university server, or personal correspondence stored on a corporate server.

As the third and fourth categories of records expand because the wealth of transactional data collected in the private sector grows and people find it more convenient to store records remotely, the legal ambiguity and lack of strong protection grows more significant and poses grave threats to privacy in the digital environment.

Congress took the first small step towards recognizing the changing nature of transactional data with amendments to the Electronic Communications Privacy Act enacted as part of the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"). But the ongoing and accelerating increase in transactional data and the detail it reveals about individuals' lives suggests that these changes are insufficient to protect privacy.

Moreover, the Electronic Communications Privacy Act must be updated to provide a consistent level of protection to communications and information regardless of where 21 they are stored and how long they have been kept. Senator Leahy's recently introduced legislation is an effort to restore Fourth Amendment protections to our personal papers. Technologies that invite us to live online will quickly create a pool of personal data with the capacity to reveal an individual's travels, thoughts, purchases, associations, and communications. We must raise the legal protections afforded to this growing body of detailed data regardless of where it resides on the network.

CONCLUSION

No doubt, privacy on the Internet is in a fragile state. Providing protections for individual privacy is essential for a flourishing and vibrant online community and marketplace. It is clear that our policy framework did not envision the Internet as we know it today, nor did it foresee the pervasive role information technology would play in our daily lives. Our legal framework for protecting individual privacy in electronic communications, while built upon constitutional principles buttressed by statutory protections, reflects the technical and social "givens" of specific moments in history. Crafting privacy protections in the electronic realm has always been a complex endeavor. Reestablishing protections for individuals' privacy in this new environment requires us to focus on both the technical aspects of the Internet and on the practices and policies of those who operate in the online environment.

However, there is new hope for the restoration of privacy. Providing a web of privacy protection to data and communications as they flow along networks requires a unique combination of tools—legal, policy, technical, and self-regulatory. We believe that legislation is an essential element of the online privacy framework and we look forward to working with this committee on the Online Privacy Protection Act (S. 809) and other proposals. Whether it is setting limits on government access to personal information, ensuring that a new technology protects privacy, or developing legislation all require discussion, debate, and deliberation. We thank the Committee for the opportunity to share our views and look forward to working with the members and 22 staff and other interested parties to foster privacy protections for the Digital Age.

[Nova Law Review, *The Internet and the Law*, Winter 1999, Volume 23, No.2, provided by Jerry Berman and Deirdre Mulligan, maintained in the Subcommittees files.]

Senator BURNS. Thank you, Ms. Mulligan. We appreciate your comments very much.

Now we have got Marc Rotenberg, director, Electronic Privacy Information Center, here in Washington, DC. Thanks a lot, Marc, for coming this morning.

**STATEMENT OF MARC ROTENBERG, DIRECTOR,
ELECTRONIC PRIVACY INFORMATION CENTER**

Mr. ROTENBERG. Thank you very much, Mr. Chairman, Senators Wyden, Rockefeller, and Bryan, for the opportunity to be here.

You probably know a bit about EPIC. We conducted the first comprehensive Web privacy survey back in 1997. And the FTC thought it was such a good idea, they did it the next year. And of course we have also been involved in a lot of the campaigns and worked with you on the encryption issue.

I would like to be able to join the chorus this morning, and tell you that self-regulation is moving in the right direction and more needs to be done, but that is not my honest view. My honest view is that self-regulation to protect privacy is much like the emperor's new clothes—everybody looks at it, says, oh, how nice, how fine, but in fact the new clothes of the emperor do not protect his privacy any more than self-regulation is protecting consumers on the Internet.

And I can point to several instances in the FTC report to try to demonstrate just how serious the problem is today. Much is made of this 66 percent number in the Georgetown survey, repeated in the FTC report, and widely cited by industry leaders as an indication of progress and success. Let me tell you what is behind that 66 percent number.

What that number says is that more and more Web sites are telling people that come to their site: We collect personal information about you and we use it for marketing and other purposes. That privacy notice, more than any other type of notice, is what people are seeing increasingly on the Internet when they go to Web sites and wonder what is happening to their personal information. And at the point that 100 percent of Web sites have that privacy notice, there is going to be very little privacy on the Internet.

The reason, simply stated, is a privacy policy is not the same as privacy protection. You can have privacy policies that say, in effect, we collect your information and do with it whatever we wish. That is our policy.

Now, it is true, of course, if you do not like that policy, you do not have to go to that Web site. And I agree with people who say, correctly, you always have the choice not to go a site that has a bad privacy policy. But, guess what? If Web sites across the Internet increasingly adopt those types of privacy policies, what is going to happen over time, people will have this choice: either to use the Internet for commerce and a whole host of other neat things that are great to do and give up their privacy, or stay off the Net. That is the choice that consumers are increasingly facing, because these privacy policies do not actually provide privacy protection.

Now, you get glimmers of this in the FTC report. At one point in the report, the FTC acknowledges that there really are not safeguards in place, that less than 10 percent of Web sites even have

the set of policies that the FTC thinks are necessary, let alone whether they are enforced—which was an issue not even considered in the FTC report, that I think should be considered—are those policies actually being followed—but then says, but let us not legislate too soon. It is a rapidly changing industry, new technology, we really do not understand it, we do not want to make a mistake; let us see how things shake out.

Let me tell you the problem with that approach. If we were talking about Y2K protection, if we were talking about the development of computer security standards, no one would say, let us wait after January 1st, and see what kind of Y2K problems we have to deal with. And if we were talking about computer security, no one would say, well, let us see how many systems are broken into and what our actual damage is before we really deal with the issue of making our systems safe to put online.

Good protection means advanced planning. It means anticipating problems and developing the policies and procedures so that the likelihood of risk, the likelihood of misuse, is reduced. And that is what privacy legislation tries to do.

It does not say to businesses, we do not want you to succeed or we want to tie your hands or you should not do neat marketing or offer great products. It says, if you are going to do these things, let us do it in a way where there are some basic privacy safeguards in place, so that people know what they are getting into when they give up personal information. If they have some problems, they have a place to turn.

I can tell you, we have had a lot of privacy legislation in this country directly in response to the development of new technologies. We did it in 1994 with the Cable Act. We did it in 1986 for the Electronic Communications Privacy Act. We have done it for auto dialers, junk faxes.

The Privacy Act of 1974, the most significant privacy law in this country, came about in part because of public concerns about the automation of records held by Federal agencies. People did not say, well, you know, we should not have a Federal Government. I mean, maybe some people said that. But they said, if we are going to automate these records, let us put in place a legal framework to protect the rights of our citizens.

I think we are in the exact same place as we approach the 21st century. We have wonderful new tools, wonderful new opportunities. Everyone agrees that the Internet is going to be a fantastic engine of economic growth. But the real choice, the critical choice in the privacy debate is, will American consumers be forced to give up their privacy as the cost of using the online services?

I think the answer to that question should be no. I think S. 809 is a wonderful, wonderful proposal. I would make some changes, but I think it is an excellent start. It sets us in the right direction to give consumers the kind of safeguards they need online, allow business to go forward, and to make sure that we do not wake up tomorrow morning and find that it is too late because privacy is gone.

Thank you very much.

Senator BURNS. Thank you very much for your comments.

Ms. Christine Varney, senior partner, Hogan & Hartson. Thank you for coming today.

**STATEMENT OF CHRISTINE VARNEY, SENIOR PARTNER,
HOGAN & HARTSON, ON BEHALF OF THE ONLINE PRIVACY
ALLIANCE**

Ms. VARNEY. Thank you for inviting me, Senator. And thank you, Senators.

I just want to put a little bit of history and perspective on the table here, and then maybe address some of the specific questions that were raised in the previous panel. I have submitted written remarks for the record, if that is all right, Senator.

Senator BURNS. Your full remarks will be made part of the record.

Ms. VARNEY. Thank you.

We have to think back to 1996, when I was at the Federal Trade Commission, and we had the first privacy workshop. And there was enormous, heated argument among most of the people in this room about whether or not you should have to tell people what information you collect online and what you do with it. And the argument was made at the time, wait a second, that is not what we do off-line; why should there be a different standard online?

I well remember sitting there with operators of a Web site, who had at the time the most popular game for 10-year-olds on the Web—and I had a 10-year-old. In order to get to the game—you could not get to the game unless you answered the following questions: How old are you? Do you have any siblings? Where do you live? Does mommy go to church? Does daddy go to church? Do you go to mommy's church? Do you go to daddy's church?

Senator BURNS. It sounds like my toaster.

Ms. VARNEY. Exactly. [Laughter.]

And the people that were running that game stood up in a room of 500 people and fully defended that practice. And I have to say, there were half the people in the room in 1996 who said, well, you know, that is the standard.

Since 1996, we have moved to a point where, in industry online, there is no serious debate. Everyone agrees that privacy is important, that consumers are entitled to know what information is collected about them, and are entitled to make choices about it.

So we have come an awfully long way in what you have pointed out is a relatively short period of time. Do we have further to go? Of course we do.

Let us look at these numbers that we have all been talking about this morning and realize what I think both Deirdre and Marc have alluded to is behind them. In the Georgetown survey, there was a finding that 66 percent of the sites that they looked at had some type of statement about data.

Well, what are the first two things that we looked at? First was did the Web site give some kind of notice? Did they explain in some way what they collected? Eighty-seven percent did.

The second thing is, did they give you some sort of choice or control, opt out, opt in? Seventy-seven percent did. Now, that is fairly high, in my view.

Where does it go down? It goes down on access. Let us be frank about access. There is a division in this country between much of industry and many leading privacy thinkers and some in government about what constitutes access.

In the Online Privacy Alliance, we believe that consumers have a right to see that data that is held about them is accurate and that one mechanism for checking accuracy can be access. We do not have a per se access requirement. And I think that is still an issue that is being debated and is evolving. I do not think we have reached a consensus—at least not commercially—on the access issue.

Security—in the study that was conducted by Georgetown, they found that of the sites that had some type of privacy notice, 44 percent had some type of security disclosed. We went back, and based only on my anecdotal checking, Senators, I can tell you, that is a failure of communication. The vast majority of Web site operators that I have talked to laughed and said, of course, we have security. This is one of our most valuable assets. We did not put it in our privacy policy. We did not know we were supposed to talk about the security which we maintain our databases in, in our privacy policy. We will put it in.

The last one is contact information. And there was a relatively low number that had the name of an individual, other than the Web master, that you could contact if you wanted information about the data that was held on you or the data practices at a company. Again, something that these companies need to work on.

About 2 weeks ago, I wrote a letter to every single Web site in our own review of the top 500 Web sites that we conducted, in connection with Ernst & Young, to every chairman of the 500 Web sites, where we could not easily find a privacy policy, and said, please, please, please, you need to tell your consumers what you are doing with their data, and you need to give them choices.

So it seems to me that the consensus you are hearing here is yes, privacy is important; how do we get there? Legislation can be one option. But I have heard from each of you different concerns. And let me tell you, in my opinion—and I know you will check with your own counsel—when Commissioner Anthony gave a detailed description of the information that someone presented to her about her family and her husband, her children, her social security number, guess what? That probably came from an entity that collected that information from public record sources. And S. 809 would probably not, in my opinion, be able to cover that.

The concerns that you have raised about cookies, Senator Bryan—unless you are at a site where you are entering your name and address, the concerns that you have raised about cookies would probably not be covered by S. 809.

So, while S. 809 reflects the goals that the Online Privacy Alliance has adopted—we have worked with your staff; these are things that we believe are important—S. 809 conflicts with the current privacy provision of H.R. 10, the banking reform bill, if that survives the conference. You would have less protection for your financial information. And financial institutions, in my reading of the two bills right now, would be largely exempt from S. 809.

So I think what you are hearing from a lot of us is let us keep working on this. It is not time to stop working. But I am just not sure that catching the bad guys and prosecuting the bad guys is going to be accomplished through S. 809 at this point in time.

Thank you very much.

[The prepared statement of Ms. Varney follows:]

PREPARED STATEMENT OF CHRISTINE VARNEY ON BEHALF OF THE ONLINE
PRIVACY ALLIANCE

The Internet is poised to become an explosive economic growth opportunity that will redefine global commerce in the information age. That growth cannot and will not occur without consumer confidence. Privacy is one of the cornerstones of consumer confidence in the Internet.

Last year numerous companies and associations came together to create policies and practices that can make privacy a reality for everyone on the Internet. These companies and associations, the Online Privacy Alliance, are pleased to submit the attached documents. First is the Mission Statement describing the goals of the Online Privacy Alliance, second are the Guidelines for Privacy Policies that will be adopted by all Online Privacy Alliance members, third are the Principles for Children's Online Activities, and fourth are the Guidelines for Effective Enforcement of Self-Regulation.

The Online Privacy Alliance has worked diligently to come up with policies that can be applied across many industry sectors. These guidelines, principles and statements reflect not only a deep commitment to online privacy, but also new policies which the Online Privacy Alliance members support. First, the Online Privacy Alliance believes that when there is use or distribution of individually identifiable information for purposes unrelated to that for which it was collected, individuals should be given the opportunity to opt out of such unrelated use or distribution. Second, the Online Privacy Alliance members believe that sites targeted at children under 13 should not engage in the collection and maintenance of information from children without prior parental consent. Finally, the Online Privacy Alliance members believe that self-regulation requires robust enforcement and they are committed to ensuring such.

Over the past year the OPA has worked to expand the adoption of effective online privacy policies by organizations doing business online. Clearly, the recent Georgetown Internet Privacy Policy Study ("The Georgetown Privacy Study") indicates that significant progress has been made in safeguarding privacy online. The fact that close to 66 percent of sites in the sample posted a privacy disclosure demonstrates that adoption and disclosure of privacy policies is becoming the norm on the Internet. Last year, the FTC reported that only 14 percent of Web sites notified consumers about their privacy policies. Although the universe from which the survey samples are drawn differ, it is very clear that there has been enormous progress.

The OPA and its supporting organizations will continue to work to ensure that effective online privacy practices are adopted and implemented among the private sector. In particular, we will be focusing on continuing outreach through business and consumer education, while increasing awareness of various privacy assurance programs. The Georgetown Privacy Study will serve as a road map to help us ensure that robust privacy practices are the norm online. It has been a pleasure working with this group and I look forward to continuing to work with the Online Privacy Alliance to build consumer confidence in the Internet.

ONLINE PRIVACY ALLIANCE

MISSION STATEMENT

The Online Privacy Alliance will lead and support self-regulatory initiatives that create an environment of trust and that foster the protection of individuals' privacy online and in electronic commerce.

The Alliance will:

- identify and advance effective online privacy policies across the private sector;
- support and foster the development and use of self-regulatory enforcement mechanisms and activities, as well as user empowerment technology tools, designed to protect individuals' privacy;
- support compliance with and strong enforcement of applicable laws and regulations;

- support and foster the development and use of practices and policies that protect the privacy of children;
- promote broad awareness of and participation in Alliance initiatives by businesses, non-profits, policymakers and consumers; and
- seek input and support for Alliance initiatives from consumer, business, academic, advocacy and other organizations that share its commitment to privacy protection.

MEMBERSHIP PLEDGE

As members of the Alliance:

- we endorse its mission;
- we commit ourselves to implement online privacy policies consistent with the Alliance's guidelines; and
- we commit ourselves to participate in effective and appropriate self-regulatory enforcement activities and mechanisms.

GUIDELINES FOR ONLINE PRIVACY POLICIES

Upon joining the Online Privacy Alliance, each member organization agrees that its policies for protecting individually identifiable information in an online or electronic commerce environment will address at least the following elements, with customization and enhancement as appropriate to its own business or industry sector.

1. Adoption and Implementation of a Privacy Policy

An organization engaged in online activities or electronic commerce has a responsibility to adopt and implement a policy for protecting the privacy of individually identifiable information. Organizations should also take steps that foster the adoption and implementation of effective online privacy policies by the organizations with which they interact; e.g., by sharing best practices with business partners.

2. Notice and Disclosure

An organization's privacy policy must be easy to find, read and understand. The policy must be available prior to or at the time that individually identifiable information is collected or requested.

The policy must state clearly: what information is being collected; the use of that information; possible third party distribution of that information; the choices available to an individual regarding collection, use and distribution of the collected information; a statement of the organization's commitment to data security; and what steps the organization takes to ensure data quality and access.

The policy should disclose the consequences, if any, of an individual's refusal to provide information. The policy should also include a clear statement of what accountability mechanism the organization uses, including how to contact the organization.

3. Choice/Consent

Individuals must be given the opportunity to exercise choice regarding how individually identifiable information collected from them online may be used when such use is unrelated to the purpose for which the information was collected. At a minimum, individuals should be given the opportunity to opt out of such use. Additionally, in the vast majority of circumstances, where there is third party distribution of individually identifiable information, collected online from the individual, unrelated to the purpose for which it was collected, the individual should be given the opportunity to opt out.

Consent for such use or third party distribution may also be obtained through technological tools or opt-in.

4. Data Security

Organizations creating, maintaining, using or disseminating individually identifiable information should take appropriate measures to assure its reliability and should take reasonable precautions to protect it from loss, misuse or alteration. They should take reasonable steps to assure that third parties to which they transfer such information are aware of these security practices, and that the third parties also take reasonable precautions to protect any transferred information.

5. Data Quality and Access

Organizations creating, maintaining, using or disseminating individually identifiable information should take reasonable steps to assure that the data are accurate, complete and timely for the purposes for which they are to be used.

Organizations should establish appropriate processes or mechanisms so that inaccuracies in material individually identifiable information, such as account or contact information, may be corrected. These processes and mechanisms should be simple and easy to use, and provide assurance that inaccuracies have been corrected. Other procedures to assure data quality may include use of reliable sources and collection methods, reasonable and appropriate consumer access and correction, and protections against accidental or unauthorized alteration.

These guidelines are not intended to apply to proprietary, publicly available or public record information, nor to supersede obligations imposed by statute, regulation or legal process.

Other valuable resources available to Alliance members in the development of privacy policies include: the OECD's "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"; the U.S. Department of Commerce's "Staff Discussion Paper of Privacy Self-Regulation"; and various industry association programs.

PRINCIPLES FOR CHILDREN'S ONLINE ACTIVITIES

The Members of the Online Privacy Alliance believe that the development of interactive online communications provides tremendous opportunities for children. At the same time, it presents unique challenges for protecting the privacy of young children. Children under 13 are special. Unlike adults, they may not be fully capable of understanding the consequences of giving out personal information online. However, children often understand how to navigate online far better than their parents do. Parents will not always have the knowledge, the ability or the opportunity to intervene in their children's choices about giving out personal information. Therefore, companies operating online must protect the privacy of children.

In connection with online activities of children under 13, the Alliance adopts the following principles.

Companies doing business online that operate sites that are directed at children under 13 or at which the age of visitors is known, must at those sites:

- Not collect online contact information from a child under 13 without prior parental consent or direct parental notification of the nature and intended use of this information, which shall include an opportunity for the parent to prevent use of the information and participation in the activity. This online contact information shall only be used to directly respond to the child's request and shall not be used to recontact the child for other purposes without prior parental consent.
- Not collect individually identifiable offline contact information from children under 13 without prior parental consent.
- Not distribute to third parties any individually identifiable information collected from a child under 13 without prior parental consent.
- Not give the ability to children under 13 to publicly post or otherwise distribute individually identifiable contact information without prior parental consent. Sites directed to children under 13 must take best efforts to prohibit a child from posting contact information.
- Not entice a child under 13 by the prospect of a special game, prize or other activity, to divulge more information than is needed to participate in that activity.

EFFECTIVE ENFORCEMENT OF SELF-REGULATION—SUMMARY

Effective enforcement of online privacy policies is intended to assure an organization's compliance with its privacy policies for the collection, use and disclosure of personally identifiable information online and provide for consumer complaint resolution. Whether administered by a third-party privacy seal program, licensing program or a membership association, the effective enforcement of self-regulation requires: (1) verification and monitoring, (2) complaint resolution and (3) education and outreach. The Online Privacy Alliance believes the best way to create public trust is for organizations to alert consumers and other individuals to the organization's practices and procedures through participation in a program that has an easy to recognize symbol or seal.

THIRD-PARTY ENFORCEMENT PROGRAMS

Validation by an independent TRUSTed third party that organizations are engaged in meaningful self-regulation of online privacy, may be necessary to grow consumer confidence. Such validation should be easily recognized by consumers, for example through the use of a seal or other symbol. The symbol or seal can be used to connote both compliance with privacy policies and an easy method for consumers to contact the seal provider. Thus, the Online Privacy Alliance supports third-party enforcement programs that award an identifiable symbol to signify to consumers

that the owner or operator of a Web site, online service or other online area has adopted a privacy policy that includes the elements articulated by the Online Privacy Alliance, has put in place procedures to ensure compliance with those policies, and offers consumer complaint resolution.

PRIVACY SEAL PROGRAM

Such a privacy seal program (hereinafter “the seal program”) should implement mechanisms necessary to maintain objectivity and build legitimacy with consumers. The seal program should utilize a governing structure that solicits and considers input from the business community, consumer/advocacy organizations and academics in formulating its policies. The seal program should strive to create a consistent and predictable framework in implementing its procedures. The seal program should be independent and should endeavor to make receipt of the seal affordable for and available to all online businesses.

A seal program should include the following characteristics:

- Ubiquity.—In order to minimize confusion and increase consumer confidence, efforts shall be taken to ensure ubiquitous adoption, and recognition of seals through branding efforts, including, for example, co-branding with corporations or associations.
- Comprehensiveness.—A seal program should be flexible enough to address issues related to both sensitive and non-sensitive information.
- Accessibility.—A seal should be easy for the user to locate, use and comprehend.
- Affordability.—The cost and structure of a seal should encourage broad use and should not be prohibitive to small businesses. The cost of a seal will vary based on a number of factors, including the extent and complexity of review, size of the business, the amount and type of individually identifiable information collected, used and distributed, and other criteria.
- Integrity.—A seal provider should be able to pursue all necessary avenues to maintain the integrity of the seal, including trademark enforcement actions.
- Depth.—A seal provider should have the ability to handle the number and breadth of consumer inquiries and complaints about the potential violation of online privacy policies and should have an established set of mechanisms to address those inquiries and complaints.

VERIFICATION AND MONITORING

A seal program must require that its participants adopt a privacy policy that comports with the principles endorsed by the Online Privacy Alliance. The scope of this requirement only applies to the participating organization and does not apply to the Web pages of affiliates or other Web pages linked to or from the participating organization’s Web page. While these baseline principles should be standardized, individual policies accepted by the seal provider should allow for sector-specific variations. The seal program must then require that an organization put in place either self-assessment or accept the seal program’s compliance review prior to awarding the seal.

If a self-assessment system is chosen, it must be pursuant to a rigorous, uniform, clearly articulated and publicly disclosed seal program methodology under which an organization would be asked to verify that its published privacy policy is accurate, comprehensive, prominently displayed, completely implemented and accessible; and that consumers are informed of the consumer complaint resolution mechanisms through which complaints are handled. A statement verifying the self-assessment should be signed by a corporate officer or some other authorized representative of the company. The self-assessment should then be reviewed by the seal program to assure compliance with the methodology. Specific criteria for when a company should improve the implementation of its self-assessment system, adopt further measures, or circumstances when a third-party review is required, should be part of the seal program’s methodology for acceptable self-assessment.

Periodic reviews should be required by the seal program to ensure that those displaying the seal continue to abide by their privacy policies and that those policies continue to be consistent with its principles. These periodic reviews may include, but are not limited to, auditing, random reviews, use of “decoys” or use of technology tools as appropriate to ensure that sites are adhering to the articulated privacy policies.

In cases where there is evidence that the company is not abiding by its privacy policies, the seal provider should establish clear criteria for placing that company on probation or beginning procedures for the seal’s revocation. The seal provider should establish clearly defined criteria for when and how a company’s seal may be revoked. A company should be given notice and the opportunity to request outside

review before its seal is revoked. Seal revocation should be a matter of public record. The seal provider must clearly state the grounds for revocation and establish a post-revocation appeals process. In addition to the above criteria, the seal provider should also strive to ensure the integrity of the seal by monitoring for misuse or misappropriation.

CONSUMER COMPLAINT RESOLUTION

An effective third-party enforcement mechanism must provide its participants and consumers a structure to resolve complaints and consequences for failure to do so. Thus, a seal program must define the scope of complaints subject to the complaint resolution process, have a system in place to address complaints, the necessary staff to handle the volume of complaints and the organizational depth to resolve them. The seal program must provide a variety of easy mechanisms to allow consumers to lodge complaints or ask questions. Seal recipients must agree to the complaint resolution procedure.

Under the complaint resolution system, consumers must first be required to seek redress for their complaints from the company they believed to have aggrieved them, before being granted access to the seal program's complaint resolution mechanism. Where complaints cannot be adequately resolved by the company, and where the consumer and company have exhausted good faith efforts to reach agreement, the company should be required to submit to a complaint resolution mechanism.

Complaint resolution outcomes must not be contrary to any existing legal obligations of the participating company. Failure of a company to agree with the outcome of the seal program's complaint resolution should result in previously identified consequences to the company. Notwithstanding the complaint resolution process, the consumer, the company and the seal provider may pursue other available legal recourse.

EDUCATION AND OUTREACH

A seal program must develop and implement policies to educate consumers and business about online privacy.

A seal program must develop and implement policies to encourage awareness of the program and online privacy issues with both consumers and businesses. Such techniques shall include: publicity for participating companies, public disclosure of material noncompliance or seal revocation, periodic publication of the results of the monitoring and review procedures, or referral of noncomplying companies to the appropriate government agencies.

ONLINE PRIVACY ALLIANCE ASSOCIATION POLICY

An association that joins the Online Privacy Alliance agrees to:

- endorse the Alliance mission statement, including: (1) adopting and posting privacy guidelines consistent with the Alliance's guidelines and appropriate to the association's membership; and (2) participating in self-regulatory enforcement mechanisms appropriate to the association's online activities;
- encourage its members to adopt privacy guidelines consistent with the Alliance's guidelines and appropriate to their industry's sector, and to implement appropriate self-regulatory mechanisms; and
- actively participate in the Alliance's business outreach and consumer education programs.

An association also may administer a seal or other third-party self-regulatory enforcement program at its discretion.

OTHER MATERIALS

- Executive Summary of the Georgetown Internet Privacy Policy Survey Conducted by Professor Mary J. Culnan. See <http://www.privacyalliance.org/resources/gipps—summary.shtml>
- Executive Summary of the OPA Privacy Policy Survey of the Top 100 Web Sites Conducted by Professor Mary J. Culnan. See <http://www.privacyalliance.org/resources/100—summary.shtml>
- Privacy Initiatives by Private Sector: A partial review of steps which OPA Supporters have done to help foster consumer confidence by protecting personal privacy in cyberspace. See <http://www.privacyalliance.org/resources/privinit.shtml>
- A Quick Guide to Helpful Tips and Technical Tools for safeguarding your privacy online. See <http://www.privacyalliance.org/resources/rulesntools.shtml>

Senator BURNS. Thank you. I appreciate that very much.

But I will have to admit that you make some very strong points when you start talking about the banking thing. We sat down and talked to some financial people, and even addressed their congressional session. And it was interesting to hear their comments, and then their comments on S. 809. Nobody said this was going to be easy to find that middle ground, but, nonetheless, we are attempting to.

Let me ask the panel if you see any difference in the online environment between this year and last year, whenever we start talking about, you know, we passed the Children's Privacy Act and now, a year later, has the landscape changed? Is there a different environment out there now? Have we learned some things? Did we do some things wrong? Did we do some things right?

I would like to hear some comments with regard to that. We will just start with you, Ms. Mulligan.

Ms. MULLIGAN. I would love to. I first want to address the Children's Online Privacy Protection Act. And, as you know, there is a rulemaking going on now. And I think, as some folks have alluded to, there are some very critical issues that have surfaced during the Commission's rulemaking. One is, for example, what does it mean to collect information in the online environment?

When you surf, you do leave behind logs that every single Web site that you visit potentially is collecting information. Now, that information, they may not be using it in any way to come back to you. They may not be interested at all in who you are. But there is just some tricky definitional issues.

And this has come up in other instances when you have dealt with how do you deal with content, and making sure that service providers, who are merely a conduit for other people's communication, are not held liable for the contents of that communication. And so there are some similar issues to look at, and make sure that you are actually placing liability on the right individuals.

And there are some other tricky issues—what is identifiable data? And one of the things that I think is very important as we look at this issue—traditionally, privacy statutes have been focused, as far as their enforcement techniques, on providing individual citizens with rights of action. The Children's Online Privacy Protection Act, the Online Privacy Protection Act that you proposed, are actually looking at a different model of enforcement and oversight, which is an FTC model.

And I think there are arguments that you can make in favor and against both of those. And one of the things that I think really needs to be explored a little bit further is which model is going to best ensure compliance, which model is going to best ensure that harmed individuals actually have some recourse, and perhaps it is a combination of the both. But I think that is an issue that really could use some more exploration. And I think this committee would serve as a useful place to have the discussion.

On the state of the Web and how things are changing, I think one of the things that we are seeing as an increasingly difficult issue and complex issue is the introduction of things that are called identifiers. This has come up with the Pentium III PSN unique identifier. And there was an enormous concern that it was going to be cookies on steroids; that this was going to provide an enor-

mous opportunity for individual's actions to be tracked and correlated all across the Web.

Another issue, which you have both raised—several members have raised—is this distinction between online and offline information. Is that something that makes sense to consumers, and is it something that actually reflects business practices? And I think that the verdict is still out on that. And I think the online environment, those lines between online and offline, while certain companies—and Jill Lesser talked about the fact that AOL does not use information about online activities in marketing to individuals or anything—that is not necessarily the norm.

And there has been a lot of discussion about a merger between DoubleClick, which makes very aggressive use of cookies, and links individuals' activities at various Web sites, which is what Senator Bryan was referring to, and Abacus, which is a very large database of people's preferences and purchasing habits at catalogs. And these two companies are merging. And what does that mean for our online and our offline identities? Are they all of a sudden going to be coming together? And what does that mean for consumers?

So there are a number of pressing issues that I think were not on the table probably 2 years ago.

Senator BURNS. Marc?

Mr. ROTENBERG. If I could, Senator, add a few additional points. I think it is important to keep in mind that over the past year there has been a critical negotiation between the United States and Europe over the future of privacy protection. And this is very important, I think, for consumers and for businesses, because it goes to the whole issue of e-commerce and transporter data flow.

And the Europeans have made clear for a long time that they feel quite strongly about the privacy issue. I think part of it has to do with the history. I think part of it also has to do with the integration of the European countries. But they said more than a year ago to the United States that we would need strong safeguards in this country for them to feel comfortable shipping private records, medical records, financial records on European citizens to the United States.

And our negotiators said, well, we thought self-regulation would do the job, and sort of reached the showdown point this past June. And the Europeans basically said, we do not think it is going to work for us. And we are seeing similar results with other countries that are moving increasingly to adopt privacy legislation. You are seeing this also, as Commissioner Anthony described, across the States. The States are not waiting. They are passing legislation. They are hearing from their voters, their consumers, that they want some safeguards now.

So I think you are seeing, one, a lot of political support and a lot of political action in support of legislation. The second thing I think you are seeing are very new business practices, with some very serious privacy repercussions. The DoubleClick-Abacus merger, which I describe in some detail in my testimony, will radically transform the nature of advertising.

Now, advertising is a very interesting marketing technique. Because it is a way for seller to reach potential customers in a segmented market and still allow people to protect their privacy. In

other words, if you are listening to a radio station or watching television or thumbing through a magazine, you are getting a lot of product information. That does not necessarily mean that the person who placed that ad or that spot knows that you are hearing it or seeing it.

Now, that could change on the Internet in a very big way. And it has to do with a point that Senator Bryan made earlier this morning. And that is the use of cookies. These cookies that sit behind the banner ads are part of a big network. It is not just the Ford site or the Eddie Bauer site or the Sears site. There are big networks, like DoubleClick, that control many of the ads that one Web surfer sees as that person goes across the Internet. And they are building elaborate profiles.

Now, DoubleClick said originally, when people started asking all sorts of questions, well, what about the privacy consequences here? They said, well, our system is going to be anonymous; we are not going to collect any personally identifiable information. And there are a thousand Web sites on the DoubleClick network that say that—anonymous, do not collect any personally identifiable information. But now DoubleClick says, we are going to merge with Abacus.

Abacus is the largest catalog database firm in the United States. And we are going to join our anonymous profiles of those people clicking Web ads with all that data that is sitting in there—profile, occupation and information—to provide you really great, high-quality, one-to-one marketing. That has enormous privacy consequences for the Internet.

And the problem right now is that we do not have a legal way to get a hold of that process. I mean, maybe, on balance, it makes sense. I do not think it does. But we need a better way to get to those kinds of issues.

Senator BURNS. Senator Bryan.

Senator BRYAN. I thank the chair. Again, a very thoughtful panel, very helpful. You have done a fine job, Mr. Chairman.

Ms. Varney, let me, if I might, just respond. I happen to be a conferee on the financial restructuring, S. 900, or H.R. 10. And, as you know, in the financial restructuring version the Senate has passed, there are no privacy provisions. We are now told that the provisions in H.R. 10, some industry folks are saying that this is a deal breaker, that these kinds of provisions will force the industry to back off.

And let me just say, I, like Senator Wyden and others, I do not have a legislative Pavlovian response that there is an issue here we have got to legislate immediately. My approach certainly would be to work as we did with AOL and direct marketers and other Web operators and the FTC to craft something, as we did with the Children's Online Privacy Protection Act. That is my approach.

But I have to tell you, this privacy issue is something that is very, very significant. With respect to banking, we now know that there are major banks—responsible, legitimate institutions—that have, in effect, without the knowledge or consent of the depositor, have transferred personal information, credit card numbers, bank account numbers, to telemarketers—some of whom are only one step away from incarceration.

Now, I think that comes as a shock to folks. So, again, I am not as sanguine, perhaps, as you are as to how we are going to get through this conference on financial restructuring.

We have a lot of States that are responding to this issue. My experience at the State level is where the Federal Government fails to act and there is perceived to be a legitimate public policy issue, the States get involved. And then we get this patchwork of legislation. Would not it make sense to have a uniform standard for the business community and the private sector, consumer advocates, to, in effect, have a baseline, as opposed to getting through a whole patchwork, if you would, of different approaches that States might take? Let me give you that question.

Ms. VARNEY. If I can just clarify. My intention in commenting on H.R. 10 was nothing other than to say it is a very difficult area. And the possible inconsistencies of H.R. 10 survive the conference with an S. 809, we have basically exempted this huge area of financial services from the requirements of S. 809. And I am also very concerned about financial data, medical data and children's data, which are generally considered to be the most sensitive kinds of data. So my comment is only to alert us to the pitfalls here.

Senator BRYAN. OK.

Ms. VARNEY. If you think back, Senator, to when the financial services industry did come to Congress and say, several years ago, we are experiencing tremendous difficulty in credit card acceptance because of the myriad of State laws, and we would like you to work with us to come up with a national law, a Federal standard, to preempt the State laws, so that we can have ubiquitous credit card deployment.

Now, some may think, in retrospect, that that is the reason we have so much personal bankruptcy, because they now send credit cards to 12-year-olds. But, on the other hand, that was an instance where industry did come to you and said, we have a problem and we have concluded that the fix is a Federal legislative fix and, with your help, we want to address it.

My sense, from the companies I work with, is that they have not excluded that. They have merely said, we are not there yet and we would like to look at technological fixes, we would like to look at the demands of the consumer in the marketplace. We want to see how all of this works.

My guess is, Senator, that many of my clients—eBay, Amazon, Yahoo, AOL—if they got to the point where they felt that individual State, possibly conflicting or inconsistent, regulation was hindering their ability to do business with consumers, they would be here in a heartbeat, asking you to work with them to fix the problem.

Senator BRYAN. Mr. Rotenberg, and perhaps Ms. Mulligan, with respect to the cookies issue, which I think, as we have talked about with the FTC panel, you do not really have a choice there. The FTC has indicated, in response to one of my questions that we really do not know the extent of the data collection. What is the correct public policy for us to pursue, either through some type of voluntary industry accord or a legislative approach? Is there any legitimate basis for them to collect information just based upon your scanning the Web?

Mr. ROTENBERG. Senator, I think the right starting point for public policy in this area is the concept of fair information practices, which the Commissioners all spoke about on the first panel. Fair information practices basically say that when a company collects some information, they have some responsibilities to you and you have some rights.

And the problems with cookies, you see, is because that data collection is so secretive; people really do not know what is going on. Now, I could describe for you many applications of cookies which are fantastic to make the Internet work.

I mean there are certain aspects of the HTTP protocol, precisely the fact that it is sort of stateless, and you come back to a Web site, having just clicked on a page, the Web site does not know who you are. So there has to be some way to sort of remember that you were the person who just clicked on the page before. And so you use cookies in these settings, for example, if you go to an online bookstore and you want to purchase something online, and you bought one book and you want to buy a second one, the company needs to know that you bought the first one. And they use cookies that way, and it makes a lot of sense.

But the banner ads which I described for you, that is a whole different thing. That is about building a profile of what you are interested in based on where you have been. And you really exercise no control.

If we took the approach that fair information practices should be enforced on the Internet, whether it is a purchase or cookies or something else, I think the rules would become clear pretty quickly. And it would be hard, for example, for Web advertisers to collect that data so secretly, but it would still be possible for Web merchants to use this same technique to fulfill a customer's order.

That is why, in my view, privacy policies actually make things simpler for people. They make it better for consumers and for businesses.

Senator BRYAN. Ms. Mulligan, any comment?

Ms. MULLIGAN. Yes, I think I would just like to elaborate. People talk about fair information practices—it is often just kind of waved about. And they are pretty simple concepts. And, as Senator Wyden stated earlier, they are pretty tried and true. They have been well tested. And basically, individuals have the right to access and correct information about them. They have the right to control how data is used that they provide to someone.

This means consent. Recordkeepers have responsibilities to tell people how they collect information, how they use information, to limit how they collect information, so that they are not collecting the extraneous information that they do not need to give you a warranty on your toaster. That they should limit the use and they should honor an individual's ability to control that data once they have collected it. That they have an obligation to maintain that data in a form that protects its quality and to provide it security. And that they have an obligation to be accountable to the public for those practices.

I think, as Mr. Rotenberg said, technology can be used in both ways that greatly advance our privacy and that advance convenience, and they can also be used in ways that undermine both indi-

viduals' expectations of confidentiality, their expectations of privacy, and kind of add to this general sense of unease, that someone is watching me.

I think that the way in which we move forward is by really looking at what are the policies that we are trying to advance, and not necessarily focusing on a specific technology—although there are technologies that I think are critically important and I think that this committee's work on encryption and the fact that we may have a bill that is looking quite strong going to the floor on the House side—I think that there is a lot of positive that technology can do, but really focusing on the technology may take our eye a little bit off the prize.

Senator BRYAN. Ms. Lesser, let me ask you a question, if I may. I catch here on the weekend newspaper that AOL—

Senator BURNS. Excuse me, Senator. Would you do me a favor and ask Senator Wyden, once he gets done with his round of questioning, could you wrap up the hearing? I have got a kind of important meeting that I have got to attend at 11:45, and I am a little late now. Can you wrap it up? Thank you very much.

Senator BRYAN. Mr. Chairman, thank you for allowing me to ask just one more question, and then I will let Senator Wyden—

Senator BURNS. You have got to deal with Wyden now. [Laughter.]

Senator BRYAN. We have already had a tradeoff here, I think, this morning.

I noticed in the Saturday paper that you are bidding farewell to these core of under-18 volunteers, who have been kind of helping you to monitor some of the activities. And I want to offer myself. In 18 months, I will be unemployed. You are saying that you are looking for someone who has greater maturity than the 15- or 16-year-olds. I am not sure that any other qualification I might have to bring to bear would have any relevancy, but I am older and more mature than the younger folks, and so I will look forward to volunteering.

Ms. LESSER. You are hired.

Senator BRYAN. I am hired. Great.

Let me ask you the question that I asked the Commissioner. That is, I thought AOL made a pretty argument, when we had the broadband frequency argument. You were talking about access and how, with the telephone network that is available, but with some of the policies being pursued by cable operators, that you did not. And that struck me. And then, I must tell you, I was somewhat surprised when you and Microsoft got into this titanic battle of the 800-pound gorillas in the industry.

Again, as I have commented earlier, Microsoft develops the technology on this instant messaging that would enable their subscribers to communicate with your subscribers, and then you developed the blocking strategy, and now they are trying to counter-block.

It strikes me that there is an inconsistency here. Let me give you an opportunity to explain that, and then I will yield to my patient friend from Oregon.

Ms. LESSER. Thank you. And I appreciate the opportunity to explain this Senator Bryan. As I think is often the case, the devil is

in the details, so let me just give you a little bit of the details, and take you back to the beginning of when we began to offer instant messaging.

It is, as you may or may not know, a technology that works somewhat like E-mail except that it pops up on your screen so it really is instant. And we developed the technology, actually, over 10 years ago. We quickly realized that it was probably the most popular item on AOL. And so what we did was we took it from being an AOL proprietary service and we made it freely available on the Internet.

So AOL Instant Messenger, which is the subject of this debate if you will, is freely available to everybody on the Internet. And over time, we have also been approached by other companies—Netscape being one before we were in discussions with our acquisition; IBM being another, that there was just a story about today where they are integrating our Instant Messenger technology into their own software, creating their own program, but basing it on our technology.

With those situations and with others that we have engaged in, we have basically a dialogue—does your technology interoperate with our technology, because we support openness and interoperability? Does it work with our technology in terms of scalability? And how does it impact our proprietary servers?

So there are lots of questions you want to ask first before you say absolutely, interconnect, have an interoperable system, we support openness. So I think it is a fundamentally consistent approach.

I will say that with respect to this hearing, I think it is an interesting issue. Because one of the things that was most distressing about the way this happened is that Microsoft did not give anybody at AOL any notice that they were going to try to interoperate, and did so just after midnight last week. And what they did, what their product does, is if you are an AOL Instant Messenger subscriber and you would go to sign up for Microsoft, it actually says, I noticed that you are a member of AOL's Instant Messaging.

So they are basically picking up the information off our server and saying to our consumers, we need your AOL screen name and your AOL password, which is a fundamental part of the way we maintain security in our system in order for you to be able to communicate through MSN's system with AOL's Instant Messenger customers.

So whereas we, every day, every time I sign on, a message comes up, saying, do not give your password to anyone and do not—and AOL employees will never ask you for your password in any situation, this sort of fundamentally undermines that security issue, and in fact looks like—the intrusion of Microsoft almost looks like the way we look at hackers. Which is, you have come in to use our technology in a way that we had no notice of.

So I think what we are going to do, moving forward, is try to work with Microsoft, with other companies that want to offer Instant Messaging and interoperate, and fully support those discussions and hope they move quickly. But, you know, I think that there are a lot of details within this particular issue that make it

more complicated and I think make it not inconsistent with the commitment to openness.

Senator BRYAN. I thank you very much. And a number of us will stay tuned in as this develops.

Ms. LESSER. Please, do.

Senator BRYAN. Thank you.

Senator WYDEN. An excellent panel. It has been a long morning, and I just have a few questions. Let me start with you, Ms. Varney.

If the chief flight mechanic for Acme Airlines admitted that he would not personally risk his life flying for Acme, Acme would obviously have a lot of problems selling tickets. Now, if 60 percent of the chief mechanics of all the airlines were surveyed, and they said, we are not going to fly because of safety concerns, the whole industry would have a lot of trouble growing their customer base.

Now, clearly, a flying accident carries more serious consequences than the violations of privacy policy. But it seems to me the online business community has a not all that different problem to my little fictional Acme Airlines. I find it absolutely astounding that 60 percent of the chief information officers, people who are in the business of making profits in this field, are unwilling to give any personal information out about themselves. I think that is what this is all about.

What I find very troubling is the good work that your companies are doing, the good work that people like me are trying to be supportive of, and stay up until the middle of the night like we did on the Y2K liability bill, to try to be supportive. I think it can really be undermined if we just sit and say, well, we will just watch all this self-regulation, and maybe it will work and maybe it will not, and we will come back when it does. I guarantee you, if there is an *Exxon Valdez* style privacy invasion, a bill will go through here like grease going through a goose. It is going to make anything that Conrad Burns and I have been talking about look like pretty small stuff.

So how would you respond to the fact that 60 percent of these people who make their living in this field will not give anything out?

Ms. VARNEY. I do not give out personal information online, Senator, ever. I do not allow my children to. I simply do not.

Now, when I go to buy office supplies or when I go to buy a book or when I go to buy an album, I look very carefully at what the privacy policies are. And I will give the information necessary to complete the transaction. And if I do not like the privacy policy, I do not shop there. I would not fly Acme.

I think the point is that there is a lot of choice. And I do not disagree with really anything you have said. I think it is an ongoing market. I think maybe the only perspective where you and I may differ slightly is, where I see the need for the debate, I do not think or recommend that you sit idly by and do nothing. I think what you are doing is exactly right.

However, I think we may be slightly premature to focus in on a particular piece of legislation for general commercial transactions. I am not talking about financial privacy, I am not talking about medical privacy, and I am not talking about kids' privacy—all of

which are highly sensitive data. I am talking about general, grown-up, commercial interactions, transactions.

We do have an obligation here—the government, the business and the consumer sections—to work together to make sure this marketplace works. Business has been doing its part. And I think it sends the wrong message to business to say, okay, you have spent the last 2 years really working hard to make privacy the norm in the online transactional environment, and now we do not think you have done the right thing, so we are going to create the norm for you. I just do not think we are there yet.

I agree with you, if the *Exxon Valdez* happens, we all better be up here and we better have our sleeves rolled up and better be prepared to deal with it.

Senator WYDEN. The problem for me is that test after test is not being met. I read Bob Pitofsky what the Commission said a year ago: Unless industry can demonstrate it has developed and implemented broad-based and effective self-regulatory programs by the end of the year, additional government authority in this area would be appropriate and necessary. It has been a year later, and I asked Bob Pitofsky if the tests were met, and he said no.

Ms. VARNEY. Well, I am not sure that I would agree with that, Senator. I think that we can talk all day, as we have been, about whether or not 14 percent to 66 percent, and everything that is underneath it, means there has been sufficient progress. Even if there were agreement that there were insufficient progress, I think you heard Ms. Lesser say that the way to go here is not a regulatory framework, it is an enforcement framework.

So I am not sure that even if we all conceded the point, we are in agreement about what to do about it. And I am certainly not willing to concede the point.

Senator WYDEN. Well, I am going to let Ms. Lesser speak for herself because she always does so very eloquently. I heard her say, and I am very comfortable with this as an orientation, that what we want to do is make sure that we have got the tools to deal with the scalawags, with the bad actors, while not weighing down people who are responsible. And that is exactly where I want to be. That is what we are trying to do with the safe harbor. As I think you know, in the discussions that we had with Senator Burns' folks, that was something I felt very strongly about, and trying to give the widest possible berth.

So I want to give you a chance to speak for yourself on this point, but I thought that the ground that you staked out there was exactly where Senator Burns and I want to be in terms of this centrist, pragmatic kind of approach, so that people who are working hard and wrestling with these issues on a regular basis, as you and a lot of your colleagues are, do not find it a burden. In fact, in almost all instances, you accede.

In fact, probably the only thing I have disagreed with at all this morning—and I think she knows that I am very fond of her—I was almost going to give Ms. Varney the chutzpah award this morning for saying, wait a minute, we have been for self-regulation, but we want to go even further on financial services and cookies than S. 809 has. And I say that in a good-natured way. And I think you made it clear that that was not what you wanted to do.

But I think we do want to strike the balance that Ms. Lesser is talking about. I want to give her a chance to speak to that point.

Ms. LESSER. Thank you, Senator Wyden. I, too, am heartened that you want to strike that balance. I am not sure that S. 809 does that the way it is drafted. And I think that, as you and I have talked about, we should continue to work not only with the industry and members of Congress, but the FTC and privacy advocates, to figure out what the baseline may be.

What I think has come out in this hearing, however—and Christine Varney did emphasize it—is that this issue is a lot more complicated than it appears on its face. Certainly requiring a notice of privacy policies gets to a fair number of problems that we are seeing online, but it does not necessarily address all the issues that people have expressed concern about.

The question really is, what are the issues that Congress should address? What are the issues that the industry should retain flexibility on? What are the issues that technology is addressing? And how do we all come together to say there may be a role for everybody?

So, as I have said before, I do not think it is wise for any company, particularly America Online, to testify that we are opposed to legislation, *per se*, because that is just not true. What we need to do is identify areas where there are—and I will maybe overqualify this—but where there are market failures. We did so, with Senator Bryan and others, in the children's bill, and we will continue to have that dialogue.

But as Deirdre Mulligan laid out very eloquently, there are many, many unanticipated issues being raised in the context of that rulemaking. We may learn from that experience, once that rulemaking is over, once the bill is actually in place, so we understand the impact on consumers, the impact on the industry, and the impact on moving forward. So I think it is an ongoing dialogue.

Senator WYDEN. Well, I think that is a fair comment.

The kind of tools we tried to put in S. 809 are ones that we think have stood the test of time, such as the principles like opt out and baseline disclosure. And as Senator Burns and I have said repeatedly, we do not think this is the last word, and we are very anxious to have your continued input.

A question for Mr. Rotenberg and Ms. Mulligan—I think you saw what I was trying to do, particularly with Chairman Pitofsky, was to try to expose some of the holes in the existing authority of the FTC to deal with these issues. I think that, by the end, he said, well, gee, we are not completely helpless, and cited a couple of examples. And I found that very helpful.

But, at the end of the day, the point that most troubles me is that if we are going to give a broad berth to self-regulation—and I made it clear that I am doing somersaults to try to do that—we have got to have some real enforcement. Both of you have made it clear that that is the Achilles heel in this self-regulation concept. I think a good way to wrap this thing up. I went to school on a basketball scholarship and you always want one shot to quit on and today I think it would be to have you two tell us what you think a good enforcement package would consist of.

Ms. Mulligan, Mr. Rotenberg, either one of you?

Mr. ROTENBERG. Senator, in the context of my comments on S. 809, one of the points that I kept coming back to was the need for the FTC to give more information to this committee and the Congress and the public about what is actually happening. I was frankly so frustrated by the FTC report, because there was no information there about enforcement, about consumer complaints. We submitted a Freedom of Information Act request to the FTC, and we have asked for all records regarding the privacy investigations, to try to understand what is going on.

But my starting point—and I think if we do it in the context of S. 809—is to have an annual reporting requirement, so that you would have information about disposition, what happens with privacy complaints, what cases were referred, how were those resolved. One of the theories underlying the self-regulatory approach, as the chairman has described, is that the FTC would operate as a backstop. If, for example, an issue could not be resolved through a self-regulatory group, like TRUSTe, then it would be referred to the FTC under Section 5 authority, and some further action can be taken.

That information has to be provided on an annual basis. You need some way to evaluate if it in fact is working.

Senator WYDEN. Ms. Mulligan, before we move on—Ms. Lesser, Ms. Varney, is that something that companies could live with? Is that kind of backstop kind of approach along the lines of something Mr. Rotenberg is talking about?

Ms. VARNEY. Well, I think in the first instance, what we are committed to at the Online Privacy Alliance is getting more companies in BBBOnline and TRUSTe and the WebTrust programs. It is an interesting discussion, Senator, that I have had with your staff and with the Commissioners. When I was a Commissioner, I believed that it could be an unfair practice to be collecting and using data without telling an individual that you are doing it, and giving them whatever rights would be concomitant with that. I continue to believe that that may be worth exploring.

Now, Bob Pitofsky was not only my professor at law school, he was also the Dean. He is far more experienced in this than I am, and he told you point blank he did not think he would win that case. But it seems to me that it is worthwhile to think about whether or not it is an unfair practice to collect data without informing individuals and giving them an opportunity to exercise control over the data.

But, in the first instance, we are committed to building the mechanisms in the marketplace.

Senator WYDEN. That actually goes beyond even what Mr. Rotenberg called for.

Mr. ROTENBERG. I will sign up for that.

Ms. LESSER. But I think what Marc is talking about and what Christine is talking about both indicate sort of a continuation of what I was talking about, which is: What are we really looking for? We are really looking to make sure consumers are protected, and that when they have complaints or problems arise or there are bad actors out there, that there is a mechanism for us to both make sure those bad actors stop engaging in business; and, second, hold them up as examples.

Because what we have seen with the FTC's enforcement actions related to their deception authority over the past couple of years has been a significant move by the industry, frankly, to a place where a good part of the industry could support the children's bill. Because we all said, despite the initial workshop on privacy which I participated in 4 years ago, that people were standing up and saying it is not necessary for us to provide parental disclosures even—forget consent—when we collect information about children—it has now really moved to be the perceived industry norm.

So I think that there is a lot that can be done in the enforcement area of the Federal Trade Commission. And it is something that you and this committee should examine.

Senator WYDEN. You can swish the last shot of the game.

Ms. MULLIGAN. OK. Well, I would like to build on a comment that Christine Varney made, and also actually a question that Marc has asked the Commission to provide documents on. I actually did file a complaint against two Web sites that were not telling consumers what they were doing with information, and were collecting incredibly detailed health information—one, targeting consumers with heart problems, collecting the most detailed list of medications, how often they take them, who prescribes them; and another very large pharmaceutical company, running a Web site aimed at asthma patients, collecting incredibly detailed information about their health, their family's health, with no disclosures of how that information was to be used, and very little acknowledgement that the company behind the Web site was in fact very large company, with many, many different interests in all different health care product industries.

Like Christine, my hope was that the FTC would in fact think that they did have jurisdiction to go after Web sites that were, I think, misleading consumers by not providing information. So, the omission rather than the act.

However, to my knowledge, there has been no action on that complaint. So I, like Christine, think that perhaps the Commission has decided that they do not have jurisdiction there, as you heard Chairman Pitofsky say.

On the question of enforcement, I think that when I look at legislative models or self-regulatory models in the privacy area, there are actually two different things that you are aiming to do. One is to instill compliance. The goal is not to have a lot of bad actors. I actually think that baseline guidance—as Commissioner Swindle said—the third of people who are not saying anything about how they handle information, you can make the assumption that they are all scalawags or you can assume that perhaps an OPA letter has not gotten to them; they do not live inside the Beltway and they are one of the 275,000 new Web sites, and that actually they would benefit from some of the knowledge that this committee has generated and that the FTC has generated, and that a little direction would go a long way.

The second part is, how do you actually get to the bad actors? And as I alluded to earlier, we have a number of statutes on the books, and most of those have looked at private rights of action as a method of enforcing. Despite the fact that I think that privacy, particularly when you are talking about sensitive information—

somebody has disclosed my medical records, I want to go in and sue, right—there is an issue as to whether or not many consumers are actually aware of the fact that their privacy has been violated.

So while I think a private right of action can be critically important for an individual's vindication, I am not certain that it is actually the best way to provide enforcement. Because, unlike the FTC, which has a fairly good pool of resources to conduct investigations, to actually go in and look at what people are doing, the average consumer, kind of the harm that is going to actually get them into court because of the expense of actually enforcing their rights, I am not sure what the right balance is between those two models. You may want a little bit of each.

But I actually think Marc's suggestion that people report is something that we have seen. It is a useful oversight mechanism, for example, in Federal wiretapping. It provides some public accountability. And I think that is critically important. But I think that looking at the remedy issue, the oversight and the enforcement issues, is something that I would like to see some more discussion on. And we are actually right now conducting some research, and I will provide it to the committee when I have some more findings.

Senator WYDEN. I still have the welts on my back from the Y2K litigation debate. So your desire to hold off on further discussion of litigation is particularly well received at this point.

Unless you all have anything to add further, know that this subcommittee, and myself specifically, having worked with all four of you very extensively in the past, really appreciates the counsel. This is by no means the last word. This is going to be a debate, as you all have said, that evolves. We are going to be working closely with all four of you, and we will excuse you at this time.

The subcommittee is adjourned.

[Whereupon, at 12:20 p.m., the hearing was adjourned.]

APPENDIX

PREPARED STATEMENT OF THE CENTER FOR DEMOCRACY AND TECHNOLOGY

BEHIND THE NUMBERS: PRIVACY PRACTICES ON THE WEB

The state of privacy on the Internet is the topic of much discussion. Much of the focus to date has been on the numbers—how many Web sites mention privacy? How many are allowing consumers the ability to opt-out? We believe it is time to focus on whether the policies in the marketplace reflect Fair Information Practices—the corner stone of information privacy—and perhaps more importantly, to decide whether they respond to consumers privacy concerns.

In considering the state of privacy protection at commercial Web sites, this report takes a three-part approach.

- First, the report reviews survey data about individuals' expectations of privacy on the Internet and in commercial interactions. The survey data suggests that adherence to the Code of Fair Information Practices on the Internet would substantially address individuals' privacy concerns.

- Second, based upon the Georgetown Internet Privacy Policy Survey data, the report further analyzes the quality of privacy policies posted by some of the most frequently trafficked Web sites. The report finds that very few Web sites are abiding by the sub-set of Fair Information Practices called for by the Federal Trade Commission.

- Third, the report examines the private sector mechanisms for overseeing and enforcing privacy polices. The report finds that the seal programs—BBBOnline, TRUSTe and WebTrust—do not require companies to comply with the full set of Fair Information Practices and, because some programs have multiple versions, individuals must read the fine print if they want to know what protections and rights the programs afford them.

The report concludes that Fair Information Practices continue to be the exception rather than the rule on the World Wide Web; private sector enforcement programs cover a very small segment of commercial Web sites; and individuals' concerns with their privacy online remain only partially answered.

1. WHAT DO WE KNOW ABOUT INDIVIDUALS' EXPECTATIONS OF PRIVACY?

Over the past four years we've witnessed an increase in surveys seeking to identify and document the public's attitudes toward privacy. Recent surveys document a growing concern with individual privacy on the Internet. Surveys have documented that the privacy of personal information is of critical concern to those on the Internet and those who have chosen not to come online. Surveys have also found a connection between individuals' willingness to engage in online commerce and their concerns with privacy. Privacy concerns continue to escalate with a recent report finding that nearly 90 percent of respondents were concerned about threats to their personal privacy online.

Privacy is becoming an increasingly important issue to Internet users

- Eighty-seven percent of Net users are concerned about threats to their personal privacy while online. (AT&T survey Beyond Concern: Understanding Net Users' Attitudes About Online Privacy, 1999)

- Privacy now overshadows censorship as the number one most important issue facing the Internet. (The 8th semi-annual poll of the Graphics, Visualization, and Usability Center at the Georgia Institute of Technology, 1997)

- Tracking people's use of the Web (32 percent), and the sale of personal information (42 percent), were cited as the most pressing privacy issues on the Internet. (Center for Democracy and Technology Privacy Survey, 1998)

- A survey of parents found that their biggest concern overall, about their children's use of the Internet, was the abuse of personal information—an issue more

troubling to them than credit card fraud, unsolicited email, and exposure to pornography and/or strangers. Sixty-five percent said that their children had been solicited to buy goods or services on the Web while more than half said their children have been asked to provide personal information at a site in order to access content. (FamilyPC Special Report: Annual FamilyPC Internet Survey Results, 1998)

Privacy concerns hinder e-commerce

- The majority of online users are not comfortable providing credit card (73 percent), financial (73 percent) or personal information (70 percent) to businesses online. (National Consumers League, Consumers and the 21st Century, 1999)
- Forty-two percent (42 percent) of those who access the Internet or the World Wide Web are using the Net only to gather information about products and services while a much smaller 24 percent are going online to purchase goods or services. (National Consumers League, Consumers and the 21st Century, 1999)
- Fifty-eight percent (58 percent) of consumers do not consider any financial transaction online to be safe, 67 percent are not confident conducting business with a company that can only be reached online, and 77 percent think it is unsafe to provide a credit card number over the computer. (National Technology Readiness Survey, conducted by Rockridge Associates, 1999)
- Many individuals have reported providing false information when registration is required. (The 9th semi-annual poll of the Graphics, Visualization, and Usability Center at the Georgia Institute of Technology, 1998)

Individuals want to know how their personal information is being used

- Very strong majorities (91 percent) of Net users, and (96 percent) of those who buy products and services online, say that it is important for business Web sites to post notices explaining how they will use the personal information customers provide when buying products or services on the Web. (AT&T survey, Beyond Concern: Understanding Net Users' Attitudes About Online Privacy, 1999)
- 66.7 percent of respondents cite the lack of information about how their personal data will be used as the reason for not filling out registration forms online. (The 10th semi-annual poll of the Graphics, Visualization, and Usability Center at the Georgia Institute of Technology, 1998)
- 41.7 percent of Internet users want to know what information is being collected and 45.8 percent want to know how it will be used before they decide to withhold or supply demographic information. (The 10th semi-annual poll of the Graphics, Visualization, and Usability Center at the Georgia Institute of Technology, 1998)
- According to another survey, the most important factor to respondents in deciding whether to provide information is whether or not information will be shared with other companies and organizations. Other highly important factors in providing information on a Web site include whether information is used in an identifiable way, the kind of information collected, and the purpose for which the information is collected. (AT&T survey Beyond Concern: Understanding Net Users' Attitudes About Online Privacy, 1999)

Individuals want control over how their personal information is used

- Eighty-seven percent of respondents objected to a Web site selling information about them to other businesses. (AARP survey "AARP Members' Concerns About Information Privacy.")
- Similar concern was registered in the context of mergers, where 71 percent of respondents believed that merging companies should obtain written permission prior to sharing information. (AARP survey "AARP Members' Concerns About Information Privacy.")
- 74.3 percent of Internet users believe that content providers (Web sites) do not have the right to resell their personal information. (The 10th semi-annual poll of the Graphics, Visualization, and Usability Center at the Georgia Institute of Technology, 1998)
- 90.5 percent of Internet users believe that individuals should have complete control over which Web sites have access to demographic information. (The survey found individuals want the control over the sale of their names and addresses by magazines to which they've subscribed.) (The 10th semi-annual poll of the Graphics, Visualization, and Usability Center at the Georgia Institute of Technology, 1998)

Internet users value their anonymity and are concerned about being tracked online

- Individuals are often very uncomfortable providing identifiable information such as credit card numbers and social security numbers. (AT&T survey Beyond Concern: Understanding Net Users' Attitudes About Online Privacy, 1999)

- 88 percent of Internet users say they value the ability to visit Web sites anonymously. (The 10th semi-annual poll of the Graphics, Visualization, and Usability Center at the Georgia Institute of Technology, 1998)
- 82.4 percent of Internet users disagree with the advertising agency practice of compiling usage behavior across Web sites for direct marketing purposes.
- Tracking people's use of the Web (32 percent) was cited as a pressing privacy concern on the Internet. (Center for Democracy and Technology Privacy Survey, 1998)

II. PRIVACY EXPECTATIONS AND FAIR INFORMATION PRACTICES

Individuals' privacy expectations, identified by the survey data above, are reflected in the Code of Fair Information Practices—broadly recognized principles designed to ensure that individuals are able to “determine for themselves when, how, and to what extent information about them is shared.”¹ Proposed in 1973 by a United States government advisory committee set up to examine the impact of computerized records on individual privacy,² the Code has never been enacted as such, but remains a sound and enduring baseline for evaluating the information handling practices of businesses and the government.³

The Code of Fair Information Practices⁴ can be summarized as follows:

Individual Rights

Access and Correction.—The individual has the right to see personal information about herself and to correct or remove data that is not timely, accurate, relevant, or complete.

Control.—The individual has the right to control the use of personal information. Personal information provided to a record keeper may not be used or disclosed for other purposes without the consent of the individual or other legal authority.

Record Keeper Responsibilities

Openness.—Record keepers who collect or maintain information about individuals must be publicly known, along with a description of the purpose and uses they make of personal information.

Limited Collection.—Record keepers who collect or maintain personal information must collect only what is necessary to support the purpose of collection. Personal information must be collected by lawful and fair means and, where appropriate, with the knowledge and consent of the individual.

Limited Use.—The use and disclosure of personal information must be limited to the purpose for which it was collected, unless the individual has granted consent.

Data Quality.—Record keepers must ensure that personal information collected is relevant to the purpose of collection, accurate, timely, and complete.

Security.—Record keepers must institute reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification and disclosure.

Accountability.—Record keepers must be accountable for complying with fair information practices.

Adherence to Fair Information Practices in the marketplace would address many of the documented privacy concerns of individuals in the online environment. The following section of the report examines the state of Fair Information Practices at commercial sites on the World Wide Web.

III. THE QUALITY OF WEB SITES' PRIVACY POLICIES

What do we know about the quality of commercial Web sites privacy policies? Do they conform to Fair Information Practices? Two surveys conducted approximately a year apart give us some information about whether Web sites are posting privacy

¹ Alan Westin. *Privacy and Freedom* (New York: Atheneum, 1967), 7.

² Report of the Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens*, U.S. Dept. of Health, Education & Welfare, July 1973.

³ Recent statements on protecting privacy from various branches of the United States government, such as the Department of Commerce's Guidelines for Effective Self-regulation, the Federal Trade Commission's 1998 Report to Congress, and the Children's Online Privacy Protection Act all center on elements of the Code.

⁴ Having discussed the Code of Fair Information Practices with many non-experts, we drafted this version in an effort to make it more accessible and self-explanatory. Comments and criticisms are welcome. For the standard text see Note 1.

policies and, if they are, what these policies say.⁵ Using the data from the most recent survey conducted by Mary Culnan—the Georgetown Internet Privacy Policy Study—we can produce some useful information about the extent to which privacy policies are being posted and how closely they align with Fair Information Practices and the sub-set of Fair Information Practices that have been called for by the Federal Trade Commission—Notice (openness); Choice (use and disclosure limitation); Access (access and correction); Security; and Enforcement (accountability).

A. Overview of the Reports

In June 1998, the Federal Trade Commission’s “Privacy Online: A Report to Congress” found that despite increased pressure, businesses operating online continued to collect personal information without providing even a minimum of consumer protection. The report looked only at whether Web sites provided users with notice about how their data was to be used; there was no discussion of whether the stated privacy policies provided adequate protection. The survey found that, while 92 percent of the sites surveyed were collecting personally identifiable information, only 14 percent had some kind of disclosure of what they were doing. Approximately 1.9 percent of Web sites provided the type of notice that the FTC considered appropriate.

The newly released Georgetown Internet Privacy Policy Survey (GIPPS) provides new data. It finds that 92.8 percent of Web sites are collecting personally identifiable information and approximately 9.5 percent of Web sites that collect personally identifiable information provide the type of notices called for by the FTC and required by the guidelines of the Online Privacy Alliance, the Better Business Bureau and TRUSTe. Approximately two-thirds of the sites made some statement about their collection or use of information—for example “your order will be processed on our secure server” or “click here if you do not want to receive email from us”—while one-third made no statements about privacy at all. The survey documented an increase in the number of Web sites collecting sensitive information such as credit card numbers (up 20 percent), names (up 13.3 percent), and even Social Security Numbers (up 1.7 percent).

B. A Closer Look at the Findings

The questions in the Georgetown Internet Privacy Policy Survey reflect a subset of Fair Information Practices. Regardless, the data provides some useful information about the state of privacy practices on the Web. The survey data suggests that 1/3 of Web sites are silent on their use of personal information while 2/3’s are taking steps toward addressing users’ privacy concerns. The policies being posted on the Web are far from complete. Less than 10 percent met the test established by the Federal Trade Commission—a sub-set of Fair Information Practice principles.

- Privacy policies are the exception not the rule on the Internet. Less than 10 percent of Web sites are meeting the standards called for by the FTC and required by seal programs.
- While data is not available, based on the GIPPS survey we believe that few Web sites are adhering to the full set of Fair Information Practices.
- A small portion of Web sites participate in self-regulatory enforcement programs. According to CDT’s analysis, only 8.5 percent of the sites surveyed (and a much smaller percentage of all sites on the World Wide Web) participate in one of the independent assessment programs discussed below.
- Roughly half of Web sites surveyed are providing visitors with some information about how personal information is collected, used, or disclosed.
- A third of Web sites are not providing individuals with any information about how personal data is handled.
- Approximately a third of Web sites surveyed are telling visitors about their use (or not) of cookies.
- Nearly 60 percent of Web sites that collect information are providing individuals the limited ability to object to its use for re-contacting.
- However, no data is available about the number of Web sites that allow individuals to limit other uses of their personal information.
- Approximately 50 percent of Web sites that collect information allow individuals to limit its disclosure to third parties.
- However, no survey data is available on whether Web sites allow individuals to limit disclosure to affiliates—a growing concern in the privacy arena.

⁵Very little data is available about whether companies are adhering to the privacy policies they post.

- Forty-five percent of Web sites inform consumers that their information is secure during transmission. But a smaller 18 percent provide security assurances for information once it is collected.

IV. PRIVACY SEAL PROGRAMS—OVERSIGHT AND ENFORCEMENT

One proposal for overseeing and enforcing privacy practices in the private sector is the use of Seal programs. Generally, the programs emphasize providing consumers with: (1) notice of a company's practices; (2) the ability to opt-out of information sharing; and (3) assurance that appropriate security is used to protect their personal information. The programs center on a contract between the seal program and the licensed seal holder. The seal is issued in exchange for the company's agreement to abide by a specific set of standards for handling personal information and to permit some form of oversight of the agreement. All use the threat of seal revocation and, in certain cases, referral to appropriate legal authorities to assure compliance.

A. Overview

CDT examined three seal programs: BBBOnline; TRUSTe; and, WebTrust. As of January 1, 2000, all of the seal programs will require licensees to comply with a similar subset of fair information principles. However, at the current time, the quality of privacy practices required of seal holders by the three programs varies substantially. Because two of the seal programs (TRUSTe and WebTrust) are in the process of raising their standards, a consumer cannot tell by the seal exactly what protections are offered. This undermines the simplicity the seals are supposed to provide.

- The BBBOnline seal relies on its well-recognized name and in-house dispute processes. The core of the BBBOnline program is a statement of compliance completed by companies and then reviewed by BBBOnline staff. BBBOnline staff initially handles disputes. If unsuccessful, the staff convenes a quasi-independent panel to hear the complaint, the findings of which are made public. Remedies for harmed consumers are decided on a case-by-case basis, but consumers cannot receive monetary damages. BBBOnline currently has 48 licensees and more than 400 applications are in process.

- TRUSTe has recently revised its license agreement. Currently, consumers cannot tell by looking at the posted seal which standard a company is abiding by, creating the potential for consumer confusion. Licenses run a range between what is called the TRUSTe 3.0 agreement, through a set of 4.0 agreements to TRUSTe 5.0. The TRUSTe 3.0 agreement assures users of little more than the fact that companies are notifying consumers of their practices. By October 1999, all of the 3.0 agreements will expire, but until January 1, 2000, when all TRUSTe licensees will be adhering to the higher (5.0) set of information practices, a TRUSTe seal could mean anything in between the 3.0 and 5.0 agreement. TRUSTe requires licensees to complete a self-certification statement that is reviewed by TRUSTe staff. To check compliance, TRUSTe seeds Web sites with personal information, conducts random spot checks of its licensees, and conducts independent audits in some instances. TRUSTe staff generally handles consumer complaints. There is no program for directly addressing the interests of aggrieved consumers. TRUSTe currently has 830 licensees and is receiving more than 100 applications a month.

- WebTrust is in the process of revising its license agreement. Currently, the license emphasizes the security of the information practices and not privacy. By December 15, 1999, all licensees will be adhering to a higher set of fair information practice. In addition to requiring a self-assessment by companies, WebTrust requires companies' policies and practices to be continually verified through on site audits by CPAs. An independent arbitration board handles disputes. The arbiter is free to award consumers with whatever remedies are considered appropriate, including money. WebTrust has awarded 22 seals and at least 40 more are in process. 150 CPA firms worldwide are able to award seals.

Do the Seal programs require Web sites to adhere to Fair Information Practice Principles?

On A Five Star Scale ★★★★★	BBBOnLine	TRUSTe 3.0 (TRUSTe has policies that range from 3.0 to 5.0. All 3.0 seals all expire by 10/99.)	TRUSTe 5.0 (Some members must follow this now, all will by 1/1/2000)	WebTrust 1.1 (All members currently follow this, beginning 9/15/1999 all members will gradually move to 2.0)	WebTrust 2.0 (All members will need to follow this by 12/15/1999)
Openness	★★★★★	★★★★★	★★★★★	★	★★★★★
Individual Participation	★★★★★	★	★★★		★★★★★
Collection Limitation	★		★		
Data Quality	★★★★★		★★★★★		★★★★★
Use Limitation	★★★		★★		★★
Disclosure Limitation	★★★		★★★		★★
Security	★★★★★		★★★★★	★★★★★	★★★★★
Accountability	★★★★★	★★	★★★	★★★	★★★

information	Yes	No	Yes	No	Yes	No	Yes	No
Security measures	Yes	No	Yes	No	Yes	No	Yes	No
Company Complaint Process	Yes	No	Yes	No	Yes	No	Yes	No
Individual Rights								
The company must provide consumers the following rights:								
The right to view personal information collected during Web site interactions held by the company.	Yes	No	Yes	No	Yes	No	Yes	No
The right to correct this information if inaccurate	Yes (must be provided online)	No	Yes	No	Yes	No	Yes	No
Access to all personal information	No							
The right to opt-out of some secondary uses of information	Yes	No	Yes	No	Yes	No	Yes	No
The right to opt-out of all secondary uses of personal information	No							
The company assumes the following obligations:								
The duty to ensure personal information is accurate, complete and timely	Yes	No	Yes	No	Yes	No	Yes	No
The duty to limit the collection of personal information to that which is necessary to complete the transaction	No (addressed in children's seal)							
The duty to protect personal information against unintended consequences	Yes	No	Yes	No	Yes	No	Yes	No
The duty to encrypt sensitive information (e.g. medical and financial information)	Yes	No	Yes	No	Yes	No	Yes	No
The duty to encrypt all personal information	No							
The duty to test for viruses	No							
The duty to ensure that third parties with whom they share data have similar security policies	Yes	No	Yes	No	Yes	No	Yes	No

The obligation to not use personal information submitted about others (such as the recipient of a package or gift) for secondary purposes	Yes (can use internal secondary purposes but not marketing nor third party sharing)	No	Yes	No	No
-------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------	----	-----	----	----

To Participate the Company must:		Yes	No	Yes	Yes (On-Site Review)	No	Yes (On-Site Review)
Complete a Pre-Registration Assessment		Yes	No	Yes	Yes	No	Yes
Agree to random checks on compliance (seeding/random reviews)		Yes	Yes	Yes	Yes	No	Yes
Agree to Quarterly Reviews of their registration		No	Yes	Yes	Yes	Yes	Yes - Quarterly
Agree to Quarterly Onsite Reviews of their policies and practices		No	No	No	No	Yes	Quarterly On-Site Reviews by licensed CPAs
If a breach of policy is identified or consumer complains:							
The company will undergo an independent audit		Yes - on a case by case basis	Yes - on a case by case basis	Yes - on a case by case basis	Yes	Yes	Yes
Harmed Consumers will be notified		Not generally. But may occur on a case-by-case basis.	Not generally. But may occur on a case-by-case basis.	Not generally. But may occur on a case-by-case basis.	Not generally. But may occur on a case-by-case basis.	Yes	Not generally. But may occur on a case-by-case basis.
Seal may be pulled if violation is not addressed or reoccurs		Yes	Yes	Yes	Yes	Yes	Yes
Proper Authorities may be notified		Yes	Yes	Yes	Yes	Yes	Yes
The company must participate in a Dispute Resolution		Yes (quasi-	No	No	No	Yes	Yes

program	independent		(Independent)		(Independent)	
	Dispute Resolutions findings are public	Yes	Maybe (case by case)	No	Maybe (case by case)	No
If an individual is found to be harmed are they compensated?	Yes (no monetary damages are awarded)	No	Yes (damages, including monetary damages may be awarded)	No	Yes (damages, including monetary damages may be awarded)	No

B. Do the Seal programs ensure compliance with Fair Information Practices? Can individuals enforce their privacy rights?

While the Seal programs' standards are, according to the GIPPS, higher than the current practices at the vast majority of Web sites, they fall short of meeting the Fair Information Practice Principles. As stated above, enforcement program participants make up only a small portion of the Web sites online. And even if a site is a member of a seal program, consumers should be wary—for today understanding what a seal means requires reading the fine print. Two sites with the same seal could have vastly different policies. While the seal programs will each have a single standard for companies to meet by January 2000, today it is clearly wise to cautious. Even with standardized requirements consumers will have to read the small print to find out the practices of a specific site and exactly what rights they may or may not have.

In addition, as a recent complaint against Microsoft filed with TRUSTe illustrated the scope of the self-regulatory enforcement programs is narrow. They only have the ability to monitor and enforce privacy practices on the companies Web site. Where a consumer has an online, but not Web site based, privacy complaint or an offline privacy complaint, the seal programs are unable to address them.

The threat of seal revocation is likely to encourage participants to more actively monitor their own behavior to ensure compliance, however seal revocation does not provide the individual who is harmed with relief. At this time it is unclear whether the private sector mechanisms for addressing consumer complaints and handling disputes will provide individuals with an effective method of protecting their privacy.

Overall, the Seal programs have raised the bar in the private sector by establishing stronger—but still short of complete—practices for handling personal information. However, they fall short of meeting the Fair Information Practice Standards and responding to consumers' concerns. Today the three programs have enrolled a total of 900 Web sites—a very small slice of the hundreds of thousand commercial sites on the World Wide Web.

V. CONCLUSIONS AND RECOMMENDATIONS

Whether the measuring tool is the policies of the Online Privacy Alliance, the seal programs, the FTC's pared down version of the Code of Fair Information Practices, or the full Code of Fair Information Practices—privacy practices at the vast majority of commercial Web sites are not making the mark.

The survey data above documented specific concerns of individuals using the Internet. In analyzing the state of privacy practices on the Web, it appears that consumers concerns are receiving an incomplete response from Web sites. Eighty-seven percent of individuals stated a concern with their privacy online—but a third of highly trafficked Web sites remain completely silent on how they handle personal information. 91 percent of Internet users, and (96 percent) of those engaged in ecommerce want to know what personal information is collected and used—but less than 50 percent of frequently trafficked Web sites provide individuals with this information. An overwhelming majority of individuals want to decide how their information is used—but 40 percent of business Web sites are not allowing individuals to exercise even a limited right to object to companies recontacting them. 74.3 percent of Internet users believe that content providers (Web sites) do not have the right to resell their personal information—but of the 53 percent highly trafficked Web sites that say they share or sell personal information less than 50 percent allow consumers to opt-out of this practice. Individuals are concerned about their use of the World Wide Web being tracked and profiled—but only 31 percent of these high traffic Web sites informed individuals about their use (or non-use) of cookies. Consumers are not being provided with adequate information about the use of personal information and they are not being provided with the ability to determine for themselves how their personal information is used.

The seal programs have improved their requirements, however they too fall short of the Code of Fair Information Practices. And together their reach continues to be quite small—covering approximately 900 Web sites. It remains unlikely that the “bad actors” will participate in self-regulatory programs. A ubiquitous oversight and enforcement program has not emerged.

In light of these statistics on the behavior of highly trafficked Web sites, consumers have good reason to be concerned for their privacy online. Thanks to the actions of leading companies, privacy and consumer advocates, and various parts of the government, some progress is evident on all fronts. However ubiquitous and enforceable privacy protections across the World Wide Web have not materialized. We continue to believe that legislation is both necessary and inevitable to make indi-

vidual privacy on the Internet the rule rather than the exception. We believe that the GIPPS survey data indicates that many Web sites need some baseline policy guidance. The relatively low participation in self-enforcement programs indicates that, on their own, they will not be a viable option for the vast majority individuals with privacy complaints. If we fail to create a privacy framework that addresses individuals' privacy concerns we stand to undermine its enormous potential to support a vital online community and marketplace.

